PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 362	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après					
Demande internationale n°	Date du dépôt inte	(Date de priorité (la plus ancienne)				
DCT /FD 00 / 00 F00			(jour/mois/année)			
PCT/FR 98/00582	20/	03/1998	11/04/1997			
Déposant						
GEMPLUS S.C.A et al.						
GEMPLUS S.C.A et al.						
Le présent rapport de recherche internation déposant conformément à l'article 18. Une						
Ce rapport de recherche internationale co	morend 2	fouilles				
Il est aussi accompagné d'une d			chnique qui v est cité.			
LAU						
<u> </u>						
1. Il a été estimé que certaines re	evendications nep	ouvalent pas faire l'objet d	l'une recherche(voir le cadre I).			
2. Il y a absence d'unité de l'inve	entlan/voir la cadra	11				
2. Il y a absence d'unité de l'inve	muon(von le caule	11).				
3. La demande internationale contrecherche internationale a été e			nucléotides oud'acides aminés et la			
dep	osé avec la demand	e internationale				
four	 i	éparément de la demande i				
<u> </u>		le la divulgation faite dans la	selon laquelle il n'inclut pas d'éléments a demande internationale telle			
tran	scrit par l'administra	tion				
	, ,	qu'il a été remise par le dép				
Le t	exte a été établi par	l'administration et a la teneu	ur sulvante:			
5. En ce qui concerne l'abrégé,						
X le te	exte est approuvé te	qu'il a été remis par le dépo	osant			
			'administration conformément à la vations à l'administration dans un délai			
d'ur	mois à compter de	la date d'expédition du prés	ent rapport de recherche internationale.			
6. La figure des dessins à publier avec	l'abrégé est la suiva	inte:				
Figure n° sug	gérée par le déposa	nt.	Aucune des figures			
pare pare	ce que le déposant i	n'a pas suggéré de figure.	n'est à publier.			
pard	ce que cette figure c	aractérise mieux l'invention.				

RAPPORT DE RECHE INTERNATIONALE

hande Internationale No PCT/FR 98/00582

A. CLAS	SEMENT	DE L	OB.	ET DE	LA DE	MANDE	
CTB 6	SEMENT)7F1	7/	32	GO	7F7/	08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement) CIB 6 G07F

Documentation consultée autre que la documentationminimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS								
Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées						
Υ	WO 93 17403 A (NSM) 2 septembre 1993	1-5,16, 23						
	voir abrégé; revendications 13-24; figures voir page 6, alinéa 2 - page 9, alinéa 1							
Υ	DE 44 27 039 A (GIESECKE & DEVRIENT) 1 février 1996 voir abrégé; revendications; figures 1,2 voir colonne 3, ligne 32 - colonne 4, ligne 41	1-5,16, 23						
Α	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 mars 1994 voir abrégé; revendications; figure voir colonne 4, ligne 8 - colonne 8, ligne 56	1-6,16,						
	-/							

X Voir la suite du cadre C pour la finde la liste des documents	Les documents de familles de brevets sont indiquésen annexe
"A" document définissant l'état général de latechnique, non considéré comme particulièrement pertinent	T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier &" document qui fait partie de la même famillede brevets
Date à laquelle la recherche internationale a étéeffectivement achevée 21 juillet 1998	Date d'expédition du présent rapport de recherche internationale 31/07/1998
Nom et adresse postale de l'administrationchargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,	Fonctionnaire autorisé David. J

RAPPORT DE PECHERCHE INTERNATIONALE

remande Internationale No

	OCUMENTS CONSIDERES COMME PERTINENTS	
atégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
	WO 96 08798 A (GEMPLUS) 21 mars 1996 voir abrégé; revendications; figures	1,2,6-23
,	EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997	
	EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994	
1	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 janvier 1997 	

IN RNATIONAL SEARCH REPORT

dormation on patent family members

iternational Application No PCT/FR 98/00582

	atent document d in search report		Publication date		Patent family member(s)		Publication date
WO	9317403	A	02-09-1993	DE AT DE EP US	4205791 132992 59301417 0628192 5557086	T D A	02-09-1993 15-01-1996 22-02-1996 14-12-1994 17-09-1996
DE	4427039	Α	01-02-1996	EP	0696021	Α	07-02-1996
EP	0589545	Α	30-03-1994	US AU AU CA	5371345 660561 4623393 2105925	B A	06-12-1994 29-06-1995 24-03-1994 18-03-1994
WO	9608798	A	21-03-1996	FR AU ZA	2724748 3475695 9507809	Α	22-03-1996 29-03-1996 07-05-1996
EP	0762333	Α	12-03-1997	JP	9297862	Α	18-11-1997
EP	0619564	A	12-10-1994	US EP AT AU CA CA CDE DE DE DE DE EP	4802218 0619563 0619565 116778 160456 160039 605443 7961287 1320578 1326911 1335839 1296809 3750958 3752138 3752138 3752138 3752146 228888 0294397 0740275	AATTTBAAAAADTDTDTAA	31-01-1989 12-10-1994 12-10-1994 15-01-1995 15-12-1997 15-11-1997 10-01-1991 24-03-1988 20-07-1993 08-02-1994 06-06-1995 03-03-1992 16-02-1995 08-06-1995 11-12-1997 26-03-1998 02-01-1998 09-04-1998 17-06-1988 14-12-1988 30-10-1996

IN RNATIONAL SEARCH REPORT

normation on patent family members

PCT/FR 98/00582

Patent document cited in search repor	t	Publication date		Patent family member(s)	Publication date
EP 0619564	А		FI JP JP NO WO US US	882047 A,B, 1500863 T 2661932 B 300660 B 8801818 A 4864618 A 4900904 A	02-05-1988 23-03-1989 08-10-1997 30-06-1997 10-03-1988 05-09-1989 13-02-1990
WO 9702547	Α	23-01-1997	NL AU EP NO	1000741 C 6613096 A 0836730 A 976151 A	08-01-1997 05-02-1997 22-04-1998 03-03-1998

TRAITE DECOOPERATION EN MATIER DE BREVETS

19/202424 PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur:	le	BUREAU	INTERNA	TIONAL
-------------	----	---------------	----------------	--------

Destinataire:

United States Patent and Trademark Office (Box PCT) Crystal Plaza 2 Washington, DC 20231 ÉTATS-UNIS D'AMÉRIQUE

Date d'expédition (jour/mois/année) 29 décembre 1998 (29.12.98)	en sa qualité d'office élu
Demande internationale no PCT/FR98/00582	Référence du dossier du déposant ou du mandataire GEM 362
Date du dépôt international (jour/mois/année) 20 mars 1998 (20.03.98)	Date de priorité (jour/mois/année) 11 avril 1997 (11.04.97)
Déposant	
ORUS, Hervé etc	
L'office désigné est avisé de son élection qui a été fa X dans la demande d'examen préliminaire inter international le:	nite: rnational présentée à l'administration chargée de l'examen préliminaire
16 noven	mbre 1998 (16.11.98)
dans une déclaration visant une élection ultér	rieure déposée auprès du Bureau international le:
L'élection	
avant l'expiration d'un délai de 19 mois à compter de à la règle 32.2b).	e la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse Fonctionnaire autorisé

Jocelyne Rey-Millet

no de téléphone: (41-22) 338.83.38

no de télécopieur: (41-22) 740.14.35

(30) Données relatives à la priorité:

97/04733

ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE Bureau international



DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ :		(11) Numéro de publication internationa	le: WO 98/47113
G07F 17/32, 7/08	A1	(43) Date de publication internationale:	22 octobre 1998 (22.10.98)

FR

(21) Numéro de la demande internationale: PCT/FR98/00582

(22) Date de dépôt international:

20 mars 1998 (20.03.98)

(71) Déposant (pour tous les Etats désignés sauf US): GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités

11 avril 1997 (11.04.97)

de Gémenos, F-13881 Gémenos Cedex (FR).

(75) Inventeurs/Déposants (US seulement): ORUS, Hervé [FR/FR]; 20, rue de la Grafounie, Zac Lou Caire, F-13470 Carnoux en Provence (FR). FOGLINO, Jean-Jacques [FR/FR]; Les Terrasses de l'Audiguier, F-13790 Peynier (FR).

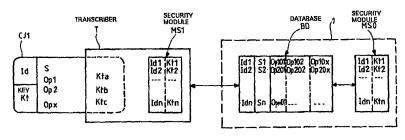
(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athelia III, Voie Antiope, F-13705 La Ciotat Cedex (81) Etats désignés: AU, BR, CA, CN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée

Avec rapport de recherche internationale.

(54) Title: SECURITY PROCEDURE FOR CONTROLLING THE TRANSFER OF VALUE UNITS IN A CHIP CARD GAMING SYSTEM

(54) Titre: PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTES A PUCE



Id...IDENTIFICATION
Op...ACCOUNT BALANCE

(57) Abstract

The invention concerns slot machines, such as jackpot or black jack and other casino gambling machines. The machines are designed to operate with gaming cards (CJ1), such as chip cards, and are connected by network to a central management unit (1). The invention is characterised in that the central management unit comprises a database (BD), wherein are stored data corresponding to those stored on the gaming cards such data concerning the gamester and card identification data (Id) and data (S, Op1, Op2) concerning the account balance stored in the card (CII). The procedure consists in verifying the card data with respect to the central management unit database to ensure the integrity of such a gambling machine system operating with chip cards or contactless cards.

(57) Abrégé

L'invention concerne les machines à sous, type jack-pot, black-jack, et autres machines de jeu d'argent de casino. Il est prévu que les machines de jeu fonctionnent avec des cartes de jeu (CJ1), type carte à puce, et sont reliées en réseau avec un organe central de gestion (1). L'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données (Id) d'identification des cartes et des données (S, Op1, Op2) renseignant sur le solde de la valeur stockée dans la carte (CJ1). Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouveille-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède								
AT Autriche FR France LU Luxembourg SN Sénégal AU Australie GA Gabon LV Lettonie SZ Swaziland AZ Azerbaidjan GB Royaume-Uni MC Monaco TD Tchad BBA Bosnie-Herzégovine GE Géorie MD République de Moldova TG Togo BB Barbade GH Ghana MG Madagascar TJ Tadjikistan BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BB Brésil IL Israël MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CH Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Pologne CN Chine KR République de Corée PT Portugal CC République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Licchtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AU Australie GA Gabon LV Lettonie SZ Swaziland AZ Azerbaidjan GB Royaume-Uni MC Monaco TD Tchad BA Bosnic-Herzégovine GE Géorgie MD République de Moldova TG Togo BB Barbade GH Ghana MG Madagascar TJ Tadjikistan BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II. Israël MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Pologne CC République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne II Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AZ Azerbaidjan GB Royaume-Uni MC Monaco TD Tchad BA Bosnie-Herzégovine GE Géorgie MD République de Moldova TG Togo BB Barbade GH Ghana MG Madagascar TJ Tadjikistan BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BJ Bénin JE Irlande MN Mongolie UA Ukraine BR Brésil IL Israël MR Mauritanie UG Ouganda BP Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Pologne CC République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
BA Bosnie-Herzégovine GE Géorgie MD République de Moldova TG l'ogo BB Barbade GH Chana MG Madagascar TJ Tadjikistan BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II. Israël MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CH Cameroun démocratique de Corée PL Pologne CN Chine KR République populaire de Corée PL Pologne CC Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne II Licchtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
BB Barbade GH Ghana MG Madagascar TJ Tadjikistan BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Greee de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil IL Israél MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République oppulaire CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Pologne CC République tchèque LC Sainte-Lucie RU Fédération de Russie CC République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Licehtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BE Belgique GN Guinée MK Ex-République yougoslave TM Turkménistan BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tohago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II Israel MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LKS Sri Lanka SE Suède	BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BF Burkina Faso GR Grèce de Macédoine TR Turquie BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tobago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II. Israél MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouveille-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CC République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne II Lichtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	вв	Barbade	GH	Ghana	MG	Madagascar	T.J	Tadjikistan
BG Bulgarie HU Hongrie ML Mali TT Trinité-et-Tohago BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II. Israël MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yongoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouveille-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	BE	Belgique	GN	Guinée	MK	Ex-République yougoslave	TM	Turkménistan
BJ Bénin IE Irlande MN Mongolie UA Ukraine BR Brésil II. Israél MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PL Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne II Lichtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	BF	Burkina Faso	GR	Grèce		de Macédoine	TR	Turquie
BR Brésij IL Israēl MR Mauritanie UG Ouganda BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LKS Sri Lanka SE Suède	BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BY Bélarus IS Islande MW Malawi US Etats-Unis d'Amérique CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
CA Canada IT Italie MX Mexique UZ Ouzbékistan CF République centrafricaine JP Japon NE Niger VN Viet Nam CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	BR	Brésil	IL	Israëi	MR	Mauritanie	UG	Ouganda
CF République centrafricaine CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun Chine KR République de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumannie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CG Congo KE Kenya NL Pays-Bas YU Yougoslavie CH Suisse KG Kirghizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CH Suisse KG Kighizistan NO Norvège ZW Zimbabwe CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazaksan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CI Côte d'Ivoire KP République populaire NZ Nouvelle-Zélande CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO ROUNAINE CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CG	Congo	KE	Kenya	NL	Pays-Bas	ΥU	Yougoslavie
CM Cameroun démocratique de Corée PL Pologne CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CN Chine KR République de Corée PT Portugal CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CI	Côte d'Ivoire	KP	République populaire	NZ	Nouvelle-Zélande		
CU Cuba KZ Kazakstan RO Roumanie CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CM	Cameroun		démocratique de Corée	PL	Pologne		
CZ République tchèque LC Sainte-Lucie RU Fédération de Russie DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CN	Chine	KR	République de Corée	PT	Portugal		
DE Allemagne LI Liechtenstein SD Soudan DK Danemark LK Sri Lanka SE Suède	CU	Cuba	KZ	Kazakstan	RO	Roumanie		
DK Danemark LK Sri Lanka SE Suède	CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
	DE	Allemagne	LI	Liechtenstein	SD	Soudan		
TV There I D Viteria CC Cinconne	DK	Danemark		Sri Lanka	SE	Suède		
FR Existing Dr Thomas 20 Studiesona.	EE	Estonie	LR	Libéria	SG	Singapour		

WO 98/47113 PCT/FR98/00582

PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTE À PUCE

La présente invention concerne le domaine des machines à sous, telles que les dispositifs de jack-pot et les autres dispositifs de jeux d'argent individuels du type de ceux que l'on trouve dans les casinos.

5

10

15

20

25

30

Elle concerne plus particulièrement des machines à sous permettant d'enregistrer des mises et des gains avec des cartes de jeu. Les cartes de jeu sont du type carte à puce ou carte sans contact. Les cartes de jeu peuvent être dédiées à cette utilisation suivant Elles sont téléphoniques. cartes l'exemple des avantageusement constituées par des cartes bancaires, d'argent sommes des transférer permettant de directement sur la machine à sous.

La présente demande vise un procédé et un système de contrôle de transfert d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant connectée à un transcripteur de données sur cartes de jeu apte à créditer et/ou à débiter des unités de valeur en mémoire d'une carte de jeu.

Un objectif général du contrôle de transfert d'unités de valeurs entre cartes de jeu et machines de jeu est d'éviter toute malversation financière à l'aide de telle cartes.

On connaît déjà des systèmes de gestion pour des machines de jeu équipées de lecteurs de cartes à puce, adaptés à la gestion d'un parc de machines de jeux disposées dans des sites relativement fermés et contrôlés comme les casinos. Ces systèmes sont adaptés à un tel environnement, car il font l'objet de contrôles et de réglementations importants, peu

5

10

15

20

25

30

susceptibles de permettre des fraudes sur les transactions de jeux utilisant des cartes à puce.

Le document EP-A-O 360 613 décrit par exemple un système de transfert de données entre carte à puce et une pluralité de machines avec des moyens de transmission et de stockage des données machine dans la carte à puce. Un tel système permet d'effectuer un relevé des opérations de jeu avec une carte de collecte stockant une liste des opérations de jeux effectuées dans un but comptable ou fiscal.

Un inconvénient d'un tel système est qu'on ne peut pas contrôler toutes les opérations de jeu effectuées, sauf à relever toutes les machines avec la carte de collecte, ce qui occasionne des manipulations fastidieuses.

D'autre part, devant la demande croissante du public, il est envisagé d'installer des machines de jeu dans des sites moins protégés que les casinos comme des salles de jeux privées ou des bars, voire même dans des lieux d'habitation privés comme le domicile des joueurs.

Il apparaît clairement qu'une telle dispersion des machines de jeu pose d'importants problèmes de sécurité des transactions suite aux opérations de jeu.

Un but de l'invention est de permettre un développement des machines de jeu fonctionnant avec des cartes à puce dans des lieux non protégés.

Un autre but de l'invention est de renforcer l'intégrité des systèmes de machines de jeux fonctionnant avec des cartes de jeu.

L'invention prévoit que les machines de jeu sont reliées en réseau avec un organe central de gestion. Selon l'invention on a prévu que l'organe central de gestion comporte une base de données, dans laquelle sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données d'identification des cartes et des données renseignant sur le solde de la valeur stockée dans la carte. Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.

5

10

15

20

25

30

L'invention prévoit ainsi un procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant connectée à un transcripteur de données sur carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :

- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification de la carte et des données représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes,
- échanger des données entre la machine et une base de gestion l'organe central données de du réseau de liaison des moyens l'intermédiaire sécurisé, notamment des données représentatives de numéro et/ou valeur unités de solde des d'identification de la carte ; et,
 - vérifier que les données en mémoire de la carte de jeu correspondent aux données de la base de données afin de contrôler l'intégrité d'un système constitué

par une telle carte, une telle machine, le réseau et l'organe central de gestion.

L'invention prévoit avantageusement des moyens de sécurisation qui permettent d'authentifier les messages de données échangées sur le réseau, c'est-à-dire de signer de tels messages.

5

10

15

20

25

30

L'invention prévoit en outre un système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, une carte de jeu stockant en mémoire des données représentatives d'opérations de jeu effectuées, notamment des données d'identification de la carte et des valeurs données représentatives de solde débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de stockant données gestion comporte une de base parallèlement en mémoire les données représentatives des opérations de jeu effectuées, notamment les données données les cartes et des d'identification représentatives des soldes des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle vérifient que, pour une carte identifiée, les données de la base et les données de la carte correspondent, notamment que les données représentatives du solde correspondent, afin de vérifier l'intégrité du système.

Un module de sécurisation pour l'authentification des messages de données peut avantageusement être prévu dans le réseau, au niveau d'un transcripteur, d'une

machine, de l'organe central, ou même des moyens de liaison du réseau.

L'invention sera mieux comprise à la lecture de la description et des dessins qui suivent, donnés uniquement à titre d'exemples non limitatifs ; sur les dessins annexés :

5

10

15

25

- la figure 1 représente un système sécurisé de contrôle de transfert d'unités de valeurs entre une pluralité de cartes de jeu et une pluralité de machines de jeu apte à mettre en oeuvre l'invention;
- la figure 2 représente un schéma d'échange et de vérification des données selon l'invention ; et,
- la figure 3 représente un calcul de certificat d'authentification par des moyens de sécurisation selon l'invention.

Sur la figure 1 on a représenté un système sécurisé de machines de jeu tel que proposé par l'invention, et qui comprend une ou plusieurs machines de jeu 200, 200', 200" et 200'".

20 Une telle machine de jeu 200, semblable aux machines à sous que l'on trouve dans les casinos dispose d'un monnayeur électronique 210 que l'on appellera par la suite transcripteur de données sur carte de jeu CJ.

Le transcripteur de données sur carte 210 est relié à l'électronique de la machine 200, par exemple par une liaison série de type RS 485. La machine et le lecteur comportent des interfaces entrée-sortie adaptées à cette liaison.

De façon classique, la machine est équipée d'un écran d'affichage 211 qui permet aux joueurs de savoir à tout instant quel est le solde dont il dispose pour jouer et le montant des mises et des gains réalisés.

La machine 200 qui a été représentée peut bien sûr électronique monnayeur à machine une être machine double à aussi une exclusivement, mais monnayeur, c'est-à-dire une machine qui comporte outre ce monnayeur électronique, un monnayeur à pièces (ou à jetons) symbolisé par la référence 201.

5

10

15

20

25

30

Dans le cas d'une machine à double monnayeur, le joueur aura la possibilité de jouer avec des pièces ou jetons et de se faire restituer ses gains uniquement sous la forme de pièces.

Les cartes de jeu CJ représentées sous forme de cartes à puce comportent une mémoire morte effaçable électriquement, par exemple une mémoire de type EEPROM.

Il peut s'agir également de cartes à puce comportant un microprocesseur, une mémoire de programmes et une mémoire de travail de type RAM.

Ces cartes à puce peuvent également être des cartes à chargement d'unités de type rechargeable. Ces cartes comportent pour cela une mémoire électriquement programmable du genre boulier.

En outre les cartes de jeu peuvent être constituées par des cartes sans contact, la carte comportant un circuit intégré à mémoire et microprocesseur, et un circuit électronique de transmission de données sans contact électrique. On peut par exemple utiliser un transpondeur tel que décrit dans la demande de brevet FR - 96 16061.

La réalisation des machines de jeu 200 et leur connexion à des transcripteurs de données sur cartes de jeu ne sera pas détaillée ici. Des exemples de réalisations de machines de jeu sont détaillés par exemple dans la demande de brevet FR - 96 10031 dont la description est incorporée à la présente.

Afin de contrôler les opérations de jeux et les transactions avec les cartes, il est prévu de relier les machines 200, 200', 200'" en réseau, avec un organe central de gestion représentés sous la référence 1 à la figure 1. Les machines du réseau sont reliées à l'organe central de gestion 1 par des moyens de liaison 123. Comme représentées à la figure 1, les machines 200, 200', 200", 200'" peuvent également être reliées entre elles par le réseau.

5

25

30

Les moyens de liaison 123 sont constitués dans le cas d'un réseau local comme celui d'un casino par une liaison locale. La liaison locale est par exemple une liaison série de type RS 485, un bus de liaison parallèle, une fibre optique, une liaison radio ou tout autre support de transmission.

Dans le cas d'un réseau joignant des salles de jeu dispersées, les moyens de liaisons peuvent être constitués par des canaux de transmission propres au réseau ou par des lignes téléphoniques.

20 Pour établir des liaisons téléphoniques, le réseau comporte des modulateurs-démodulateurs de type MODEM 120, 120', 120" et 120"', disposés en interface entre les moyens de liaison 123 et une machine de jeux 200, 200', 200", 200"' respectivement.

L'organe central de gestion 1 est constitué par exemple d'un ordinateur central relié également aux moyens de liaison 123 par un MODEM 101 de façon à faire partie du réseau.

Sur la figure 1 on a représenté des moyens de liaison 123 sous la forme schématique d'une ligne annulaire à laquelle les machines de jeux 200, 200', 200" et 200" sont connectées. Les machines sont ainsi reliées entre elles et à l'organe central de gestion 1.

La liaison peut cependant prendre toutes sortes de formes équivalentes.

Dans le cas de liaisons téléphoniques, les machines sont reliées individuellement aux moyens centralisés de gestion, les machines n'étant pas nécessairement reliées entre elles. Le MODEM 101 des moyens de gestion 1 peut comporter avantageusement un standard de plusieurs lignes téléphoniques.

5

10

15

20

25

30

L'utilisation de liaisons téléphoniques présente l'avantage de permettre d'étendre le réseau au lieu d'habitation des joueurs. Les machines de jeux sont de préférence constituées par des ordinateurs personnels 300 et 300' de type PC. Les machines peuvent ainsi être connectées chacune à un transcripteur de données sur carte de jeu 310 ou 310' intégrant de préférence un MODEM 130 ou 130', par exemple du type "GEMTEL" commercialisé par la demanderesse.

Le réseau utilisé peut être notamment un réseau de communication ouvert du type "INTERNET".

Il est prévu en outre que le système et le réseau comportent au moins un terminal de chargement représenté à la figure 1 sous forme d'une caisse enregistreuse 100. Le terminal de chargement 100 comporte alors un transcripteur 110. Le terminal 100 et le transcripteur 110 sont alors reliés au réseau par l'intermédiaire d'un MODEM 111 connecté aux moyens de liaison 123.

Classiquement, il est prévu que les cartes à puce dédiées aux jeux sont des cartes non-rechargeables, à l'instar des cartes téléphoniques, et elles sont fabriquées et chargées uniquement par un organisme central.

Dans une application avec des cartes nonrechargeables, il est prévu que la base de données BD des moyens centralisés de gestion 1 dispose des soldes S1, S2, ..., Sn initiaux des valeurs créditées sur les cartes CJ1, CJ2, ..., CJn avant leur mise en circulation.

Cependant, selon une variante avantageuse, il est prévu que les cartes sont rechargées en unités de valeurs par l'intermédiaire de terminaux de chargement.

5

10

15

20

25

30

En pratique, ce terminal peut être celui d'un caissier du casino. De façon alternative, on peut prévoir une multitude de terminaux de chargements disposés dans des débits de tabac ou dans d'autres commerces accessibles aux joueurs.

Ainsi lorsqu'un joueur désire obtenir la délivrance d'un crédit, il donne sa carte de jeu CJl à l'opérateur habilité à utiliser le terminal 100 qui insère cette carte dans la partie transcripteur 110 de ce terminal 100 et qui au moyen du clavier de la caisse va rentrer le montant du crédit que désire avoir le joueur. Ce montant est transféré au transcripteur 110 qui enregistre alors sur la carte à puce CJl l'information significative correspondant au crédit désiré par le joueur.

Selon l'invention, le terminal de rechargement peut alors communiquer à l'organe central de gestion 1, par l'intermédiaire des moyens de liaison du réseau 123, les données lues sur la carte à recharger, notamment son numéro d'identification Id et son solde S d'unités de valeur. La vérification du numéro d'identification Id de la carte de jeu CJ1 peut être faite directement par le terminal de rechargement 100 ou par son transcripteur de données 110 ou de manière alternative par l'organe central de gestion 1. L'invention prévoit ainsi une étape préliminaire aux opérations de jeu, consistant à inscrire dans la base de données de

l'organe central de gestion 1 et dans la mémoire d'une carte de jeu CJ1, des données représentatives d'une valeur de solde initial lors d'une opération préliminaire de chargement de la carte CJ1.

5

10

15

20

25

30

Selon la première alternative, il est prévu comme visible à la figure 2 que le terminal de rechargement dispose des transcripteur ou d'identification secrètes Kt1, Kt2, ..., Ktn de toutes les cartes de jeu CJ1, CJ2, ..., CJn en circulation. Ces clés secrètes sont de préférence stockées dans un module de sécurisation MS1 comportant une mémoire et une unité de calcul, les données stockées n'étant pas accessibles de l'extérieur. Le terminal 100 vérifie alors que l'identification Id1 de la carte à puce CJ1 est correcte avec la clef Kt1 correspondante, appliquant un algorithme d'authentification cryptage selon les méthodes connues.

alternative, seconde la authentification de la carte est effectuée au niveau de numéros les 1, gestion central de l'organe clefs les Id1, Id2, ..., Idn et d'identification d'authentification correspondantes Kt1, Kt2, ..., Ktn étant stockées dans la base de données BD de l'organe central de gestion ou de préférence dans un module de sécurité MSO similaire à MS1. Cette seconde alternative présente l'avantage d'éviter toute dissémination des clefs d'authentification secrètes.

L'invention prévoit en outre un échange de données entre le terminal et l'organe central de gestion portant sur les données stockées dans la base de données de l'organe central de gestion 1. De préférence, cet échange de données est accompagné d'un certificat d'authentification. Un protocole de sécurisation permettant d'émettre de tels certificats

5

10

15

20

25

30

protocole ci-après. Ce détaillé sera avantageusement qu'une machine parasite du réseau ne crédite abusivement la base de donnée. Le terminal T peut ainsi communiquer le solde S des valeurs débitées et/ou créditées précédemment sur la carte de jeu CJ1 à l'organe central de gestion 1. Après avoir authentifié le numéro d'identification Id1 de la carte ou le certificat accompagnant les données de solde, on peut ainsi vérifier que le solde S inscrit en mémoire de la carte de jeu CJ1 correspond bien au solde S1 stocké dans la base de données BD. Si la vérification est positive, il est prévu que l'organe central de gestion 1 émet un signal d'accord pour le rechargement de la carte CJ1 par le terminal et le transcripteur T. En cas de vérification négative, une procédure ou un signal d'alerte peuvent être mis en oeuvre au niveau de l'organe central de gestion 1, ou au niveau du terminal de chargement. Dans un réseau de machines à sous de casino par exemple, le caissier pourra être alerté par le terminal de chargement afin de découvrir l'origine d'un tel dysfonctionnement. Dans un réseau plus étendu, on peut prévoir que la carte CJ1 soit avalée par le transcripteur T du terminal afin d'enquêter sur le dysfonctionnement.

On peut prévoir en outre que la base de données ou la mémoire des cartes de jeu CJ comportent des informations sur le joueur, par exemple sur son âge, ses habitudes de jeu pour des applications de fidélisation des joueurs, de remise de parties gratuites, etc.

Nous allons présenter maintenant des protocoles de contrôle de transferts d'unités de valeur au cours d'opérations de jeu effectuées avec le procédé ou le système selon l'invention.

Au début des opérations de jeu, le transcripteur de données sur carte 210 de la machine de jeu lit le numéro d'identification en mémoire de la carte de jeu CJ1. Comme exposé précédemment au vu de la figure 2, ce préférence de est d'identification Id authentifié par un module de sécurité MS1 prévu dans le transcripteur T. Le numéro Id peut éventuellement être communiqué à l'organe central de gestion 1 en vue clef avec 1a CJ1 d'authentifier carte ٦a module dans le d'identification Kt1 contenue sécurité MSO. Cette étape d'identification est préférence effectuée une seule fois pour plusieurs opérations de jeu avec la même carte sur la même mémorisant terminal le ou machine la machine, éventuellement ce numéro d'identification Id pour les opérations suivantes.

5

10

15

20

25

30

A chaque opération de jeu suivante, le solde S des unités de valeur affecté au joueur est revu à la suite des mises ou des gains réalisés.

réalisation de mode premier un Selon l'invention, il est prévu de communiquer simplement à l'organe central de gestion 1 des données relatives à l'opération de jeu effectuée, notamment le nouveau solde d'unités de valeur obtenu au cours de cette opération de jeu. L'organe central de gestion 1 peut ainsi stocker la liste des opérations effectuées, sous forme d'une liste des crédits ou des débits successifs liste CJ1. Cette la carte sur enregistrés opérations Op101,Op102,..., Op10x est par exemple enregistrée dans la base de données BD sous le numéro CJ1 carte Id1 de la d'identification d'utilisation.

La recopie du solde S1 ou des opérations Op101, Op102, ..., Op10x dans la base de données BD de

l'organe central de gestion 1 sert alors à établir un relevé comptable des opérations ou à effectuer des vérifications fiscales. Un tel historique des opérations permet également lors d'une vérification d'une carte falsifiée de mesurer l'étendue de la fraude.

5

10

20

25

Selon un deuxième mode de réalisation de l'invention, il est prévu une étape supplémentaire consistant à vérifier que les données en mémoire de la carte CJ1 et les données de la base de données BD correspondent afin de contrôler l'intégrité d'un système constitué par une telle carte CJ1, une telle machine 200, le réseau 123 et l'organe central de gestion 1.

Deux types de vérification peuvent être prévues, la vérification pouvant porter sur le numéro d'identification Id ou sur le solde S de la carte.

La vérification du numéro d'identification Id1 de clé une avec effectuée CJ1 est carte d'identification Kt1 comme on l'a vu précédemment. Selon ce deuxième mode de réalisation, d'identification Id est communiqué à l'organe central 1 via les moyens de liaison 123 du réseau. L'organe central 1 stocke les clés d'identification Kt1, Kt2, ..., Ktn des cartes CJ1, CJ2, ..., CJn en circulation, dans sa base de donnée BD ou de préférence dans un module de sécurisation MSO. Le module de sécurisation MSO effectue ainsi les calculs d'identification en interne.

De plus, la vérification peut porter sur le solde d'unités de valeur de la carte CJ1. Dans ce cas, le transcripteur T lit sur la carte les données de solde S des unités de valeur et les envoie à l'organe central de gestion 1 par l'intermédiaire des moyens de liaison

du réseau 123. La vérification du solde S de la carte CJ1 est alors effectuée par rapport au solde S1 indiqué sous le données BD de base la dans deux soldes S et S1 d'identification Idl. Si les correspondent, l'opération de jeu est autorisée par l'organe central de gestion 1.

5

10

15

20

25

30

Selon une autre alternative, la vérification peut porter sur la certification des données échangées à partir de la carte de jeu CJ1. Des algorithmes standards d'encryptage de données type algorithme DES permettent en effet de certifier les données numériques échangées entre la carte CJ1, le transcripteur T, la machine de jeu et l'organe central de gestion 1. Le cryptage et le décryptage du certificat accompagnant les données transmises n'est possible et cohérent que si on utilise une clé secrète.

Les algorithmes de cryptage de donnés de type DES comportent des séries de calculs complexes qui ne seront pas détaillés dans la présente.

Un exemple de mise en oeuvre d'algorithme DES sera exposé en considérant simplement que l'algorithme fournit un nombre crypté, appelé clef de session K', à partir d'un premier nombre donné, appelé clef d'identification K et d'un nombre aléatoire Rnd, selon l'exemple de la formule suivante :

K' = DES(K, Rnd)

La complexité des algorithmes DES rend impossible la découverte d'une clef d'identification secrète K à partir de la clef de session K' et du nombre aléatoire Rnd.

La figure 3 montre un exemple d'application d'un algorithme DES. Il permet d'illustrer des moyens de sécurisation du réseau, en particulier la sécurisation

des échanges de données effectuées via les moyens de liaison du réseau. La carte de jeu dispose dans une zone mémoire inaccessible d'au moins une clé d'identification secrète Kt. Le microprocesseur de la carte génère un nombre pseudo aléatoire Rnd1. A partir de ces deux nombres Rnd1 et Kt, l'algorithme DES mis en oeuvre par le microprocesseur calcule une clef de session Kt'.

5

10

15

20

25

30

Cette clef de session Kt' peut servir de certificat d'authentification et être envoyée avec le nombre aléatoire Rnd1 et les données à certifier. Cependant, pour rendre toute découverte des clefs impossible, il est prévu d'appliquer une seconde fois l'algorithme DES. Comme visible figure 3, la carte de jeu, organe émetteur du message à certifier, demande à l'organe destinataire, l'organe central 1 par exemple, de lui fournir un second nombre aléatoire Rnd2.

L'algorithme DES est à nouveau appliqué à la clef de session Kt' et au second nombre aléatoire Rnd2 par le microprocesseur de la carte pour calculer un certificat C.

Le message de données est alors envoyé à l'organe destinataire accompagné du certificat C et du nombre aléatoire Rnd1 calculés par la carte. Ainsi les clefs utilisées, en particulier la clef d'identification secrète Kt, ne sont pas échangées.

de données message L'authentification du effectué en recalculant un certificat C' à partir des même données. L'organe central de gestion 1 dispose la de sécurisé MSO module son dans d'identification secrète Kt. Le module sécurisé MSO peut donc calculer la clef de session Kt' à partir de la clef d'identification Kt et du nombre aléatoire Rnd1.

Le module sécurisé MSO dispose encore du nombre aléatoire Rnd2 qu'il a fourni précédemment à la carte de jeu. A partir de ces deux nombres Rnd2 et Kt', le module de sécurité MSO calcule à nouveau un certificat C' en appliquant une seconde fois l'algorithme DES.

5

10

15

20

25

30

En vérifiant que le certificat C calculé par la carte correspond au certificat C' recalculé par son module de sécurité, l'organe central peut authentifier le message de donnée recu.

Notons que la clé de session Kt' et le certificat C sont recalculés à chaque certification de message désirée. On évite ainsi que une machine pirate du réseau obtienne l'accès à la base de donnée ou à la mémoire de la carte en recopiant une certification précédente.

Après avoir effectué une ou plusieurs de ces vérifications, l'organe central 1 envoie un signal d'accord qui peut être crypté ou encodé. Avec un tel signal d'accord, le joueur peut utiliser sa carte de jeu CJ1, effectuer des mises, des opérations de jeu et recharger sa carte avec ses gains.

Dans ces deux premiers modes de réalisation, on a vu que la carte a une fonction d'identification, son numéro Id permettant à l'organe central 1 ou à la machine de jeu de la reconnaître voire de reconnaître le joueur dans certaines applications de fidélisation de clientèle. De plus, la carte a une fonction de porte-monnaie, le solde d'unités de valeur étant stocké dans la carte et connu essentiellement par la carte, la recopie de solde dans l'organe central 1 servant aux fins de vérification.

Selon un troisième mode de réalisation, la fonction porte-monnaie n'est plus assurée par la carte mais par l'organe central de gestion lui-même. La carte

ne comporte alors aucune donnée relative au solde du joueur mais uniquement des données d'identification, telles que le numéro d'identification Id, plusieurs clefs Kta, Ktb, Ktc d'authentification et éventuellement des informations sur le joueur. Les données de solde S1 des unités de valeur sont alors uniquement stockées dans la base de données BD de l'organe central de gestion 1. Ce compte d'unités de valeur se trouve par exemple dans la base de données sous le numéro d'identification Id1.

5

10

15

20

25

30

Lors d'une opération de jeu, le numéro d'identification Id de la carte CJ1 est envoyé à l'organe central de gestion 1 via les moyens de liaison 123 du réseau. Le numéro d'identification Id peut être envoyé directement par la machine de jeu 200 ou par son transcripteur 210 s'il a été mémorisé par la machine ou par son transcripteur. Le numéro d'identification Id peut aussi être lu sur la carte et envoyé à l'organe central de gestion 1 par le transcripteur 210 à chaque opération de jeu.

Après vérification du numéro d'identification Id, l'organe central de gestion 1 consulte la base de données BD et envoie à la machine de jeu 200 le solde S1 des unités de valeur affecté à la carte CJ1.

De préférence le transfert des données de solde d'unités de valeur est effectué avec un certificat selon le protocole de sécurisation des échanges de données présenté précédemment.

Un avantage de ce troisième mode de réalisation est que les montants mis en jeu sont stockés dans l'organe central de gestion 1, ce qui évite toute mémorisation de valeur au niveau des cartes de jeu.

Selon ce troisième mode de réalisation, il est donc prévu de stocker, dans la base de données des

moyens centralisés de gestion, les données représentatives du solde des valeurs débitées et/ou créditées afin d'éviter une fraude à partir d'une carte à puce.

5

10

15

20

25

30

Le contrôle consiste simplement dans ce troisième mode de réalisation à vérifier le numéro d'identification Id de la carte de jeu CJ1 avec une clé d'identification Kt1 lue dans la base de données BD de l'organe central de gestion 1 afin de contrôler l'intégrité de la carte.

Avec ces trois modes de réalisation de l'invention on a vu qu'on peut avantageusement contrôler l'intégrité des cartes de jeu utilisées sur les machines de jeu.

De plus, en mettant en oeuvre des moyens de sécurisation des échanges de données, l'invention permet avantageusement de vérifier l'intégrité d'un système formé par les cartes de jeu, le réseau de machines de jeu et la base de données de l'organe central de gestion, l'intégrité d'un des trois éléments du système, soit une carte de jeu, soit le réseau, soit la base de données étant vérifiée à l'aide des deux autres éléments.

L'invention prévoit en effet un système apte à mettre en oeuvre le procédé selon l'invention.

Un tel système comporte une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau avec un organe central de gestion par l'intermédiaire de moyens de liaison.

Selon l'invention, les données représentatives des opérations de jeu effectuées avec une carte à puce sur une machine de jeu sont stockées en mémoire de la carte

de jeu et parallèlement dans une base de données prévue dans l'organe central de gestion.

Les données stockées sont notamment les données d'identification de la carte et le solde ou les soldes successifs d'unités de valeur débitées et/ou créditées avec la carte.

5

10

15

20

25

30

Des moyens de contrôle tels qu'un programme d'ordinateur effectuant l'authentification du numéro d'identification de la carte ou la comparaison des valeurs de solde stockées sur la carte et dans la base ou encore la certification des données échangées sont prévus afin de vérifier l'intégrité du système.

De préférence, pour sécuriser les échanges de données sur le réseau, il est prévu qu'un module de sécurisation calcule un certificat d'authentification à partir de données secrètes stockées en mémoire du module et en ce que les moyens de contrôle vérifient que le certificat d'authentification calculé par le module de sécurisation correspond au certificat d'authentification calculé par la carte de jeu ou par un autre module de sécurisation.

De tels modules de sécurisation MSO, MS1 peuvent être disposés dans les cartes du jeu CJ1, CJ2, ..., CJn, ou au niveau des transcripteurs 10, 110, 210, 210', 210'', 210''', 310, des machines de jeu 200, 200', 200'', 200''', de l'organe central de gestion 1 ou même sur les moyens de liaison 123 du réseau.

On peut en particulier prévoir plusieurs modules ou des moyens répartis de sécurisation au sein du réseau. Chaque transcripteur 10, 210, 210', 210", 210", ou chaque interface 11, 120, 120', 120", 120"' comprend par exemple un module de sécurisation de sorte que les échanges de données sur les moyens de liaison 123 son accompagnés de certificat d'authentification.

Par exemple le transcripteur 10 émetteur ajoute à son message son certificat qui est authentifié par le transcripteur 210 destinataire avant d'être transmis à la machine 200 correspondante.

D'autres variantes de réalisation, avantages et caractéristiques de l'invention, apparaîtront à l'homme du métier sans sortir du cadre des revendications ciaprès.

5

5

10

15

30

REVENDICATIONS

- 1. Procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ, CJ1, CJ2, CJn) et une pluralité de machines de jeu (200, 200', 200'', 200''', 300, 300', 300"), chaque machine étant connectée à un transcripteur (210) de données sur carte de jeu (CJ2), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :
 - lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification (Id) de la carte (CJ1) et/ou des données (S, Op1, Op2, Opx) représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes, le procédé étant caractérisé en ce qu'il comporte des étapes consistant à :
- échanger des données entre la machine (200) et une base de données (BD) de l'organe central de gestion (1) par l'intermédiaire des moyens de liaison (123) du réseau sécurisé, notamment des données représentatives de solde (S) des unités de valeur et/ou le numéro d'identification (Id) de la carte ; et,
 - vérifier que les données en mémoire de la carte de jeu (CJ1) correspondent aux données de la base de données (BD) afin de contrôler l'intégrité d'un système constitué par une telle carte, une telle machine, le réseau et l'organe central de gestion.
 - 2. Procédé selon la revendication 1, caractérisé par une étape préliminaire aux opérations de jeu, consistant à :

PCT/FR98/00582 WO 98/47113

- inscrire, dans la base de données (BD) de l'organe central de gestion (1) et dans la mémoire d'une carte de jeu (CJ1), des données représentatives d'un solde (S, S1) initial d'unités de valeur lors d'une opération préliminaire de chargement de la carte. revendications des l'une selon Procédé précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :
- inscrire, dans la base de données (BD) données gestion (1), des central de 10 représentatives du solde (S1) des unités de valeur de la carte de jeu (CJ1).

5

15

25

30

- revendications des selon l'une Procédé 4. précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :
- recevoir les données représentatives du solde (S1) des unités de valeur à partir de l'organe central de gestion (1) afin d'éviter une fraude à partir d'une carte (CJ2) ou d'une machine de jeu (200).
- revendications des l'une selon Procédé 20 ce que l'étape caractérisé en précédentes, vérification consiste à :
 - vérifier les données représentatives de solde (S) des unités de valeur lues en mémoire de la carte de jeu (CJ1) par rapport aux données (S1) lues dans la base de données (BD) afin de contrôler l'intégrité de la carte de jeu (CJ1).
 - revendications des selon l'une Procédé l'étape de caractérisé ce que en précédentes, vérification consiste à :
 - vérifier le numéro d'identification (Id) de la carte de jeu (CJ1) avec une clé d'identification (Kt1) lue dans la base de données (BD) de l'organe central de

5

10

15

20

25

30

PCT/FR98/00582 WO 98/47113 23

gestion (1) afin de contrôler l'intégrité de la carte de jeu (CJ1).

- Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation (MSO), le procédé comportant une étape supplémentaire consistant à :
- prévoir que les moyens de sécurisation (MSO) du réseau calculent un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des moyens de sécurisation.
- Procédé selon la revendication 7, caractérisé par une étape supplémentaire consistant à :
- certificat d'authentification lire un calculé par la carte de jeu (CJ1) à partir de données secrètes (Kt, Kt1) en mémoire de la carte.
- Procédé selon la revendication 8 caractérisé en ce que l'étape de vérification consiste à :
- vérifier que le certificat d'authentification (C) calculé par la carte de jeu (CJ1) correspond au certificat d'authentification (C') calculé par les moyens de sécurisation (MSO) du réseau.
- 10. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation répartis (MSO, MS1), le procédé comportant des étapes supplémentaires consistant à :
- prévoir que des premiers moyens de sécurisation du réseau calculent un premier certificat (MS0) d'authentification (C') à partir de données secrètes premiers moyens des mémoire en Kt') sécurisation (MSO), et
- prévoir que des seconds moyens de sécurisation second réseau calculent un (MS1) d'authentification à partir de données secrètes en mémoire des seconds moyens de sécurisation (MS1), et

5

10

15

25

30

- vérifier que le premier certificat d'authentification (C') calculé par les premiers moyens de sécurisation (MSO) du réseau correspond au second certificat d'authentification calculé par les seconds moyens de sécurisation (MS1) du réseau.
- 11. Procédé selon l'une des revendications 7 à 10 caractérisé en ce que les données (Id, S) échangées entre la machine (200) et la base de données (BD) de l'organe central de gestion (1) sont accompagnées d'un certificat d'authentification (C, C').
- 12. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés au transcripteur (T, 10, 110, 210) de données sur carte de jeu (CJ1) afin de contrôler l'intégrité d'une telle carte.
- 13. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés à une machine de jeu (T, 200, 300).
- 14. Procédé selon l'une des revendications précédentes 20 caractérisé en ce que des moyens de sécurisation sont associés aux moyens de liaison du réseau.
 - 15. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS0) sont associés à l'organe central de gestion (1) afin de contrôler l'intégrité du réseau.
 - Système sécurisé de contrôle de d'unités de valeur entre une pluralité de cartes de jeu (CJ) et une pluralité de machines de jeu (200, 300), chaque machine étant pourvue d'un transcripteur (210, 310) apte à débiter des unités de valeur d'une carte de jeu (CJ), les machines étant reliées en réseau sécurisé organe central de gestion (1) l'intermédiaire de moyens de liaison (123), une carte de jeu (CJ1) stockant en mémoire des données (S, Op1,

représentatives d'opérations (xqO Op2, effectuées, notamment des données d'identification (Id) de la carte et des données représentatives de solde (S) des unités de valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce 5 que l'organe central de gestion (1) comporte une base de données (BD) stockant parallèlement en mémoire les données (S1, Op101, Op102, Op10x) représentatives des opérations de jeu effectuées, notamment les données d'identification (Id1, Id2, Idn) des cartes et 10 données représentatives des soldes (S1, S2, Sn) unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens vérifient que, une pour contrôle (BD) identifiée, les données de la base (BD) et les données 15 de la carte (CJ1) correspondent, notamment que les données (S, S1) représentatives du solde d'unités de valeur correspondent, afin de vérifier l'intégrité du système.

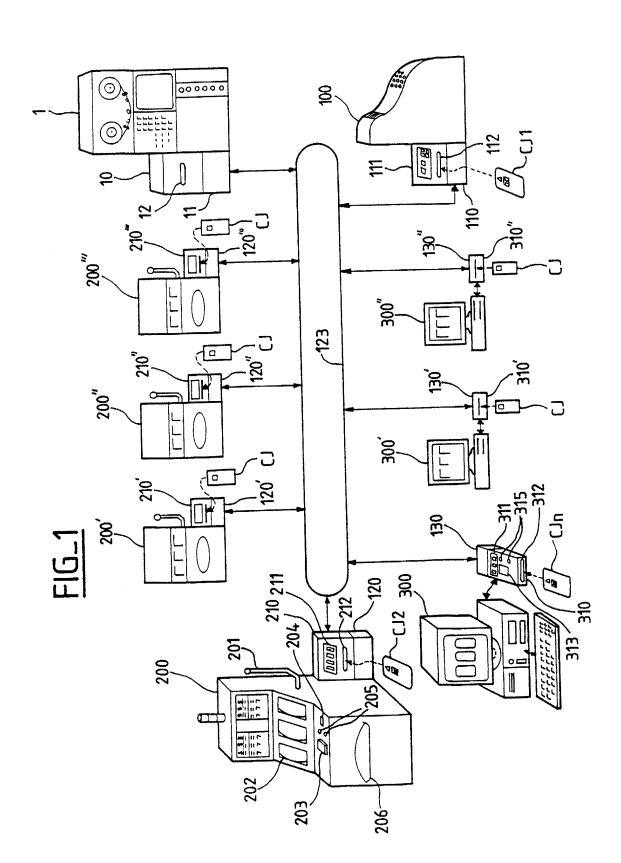
- 17. Système sécurisé selon la revendication 16, caractérisé en ce que la carte de jeu (CJ1) calcule un certificat d'authentification (C) à partir de données secrètes (Kt, Kt') stockées en mémoire de la carte (CJ1).
- Système sécurisé selon la revendication 16 ou la 25 revendication 17, caractérisé en ce qu'il comporte en outre au moins un module de sécurisation (MSO, MS1), le certificat calculant un sécurisation d'authentification (C') à partir de données secrètes (Kt, Kt') stockées en mémoire du module (MSO) et en ce 30 que les moyens de contrôle (MSO) vérifient que certificat d'authentification (C') calculé par certificat correspond au sécurisation de module

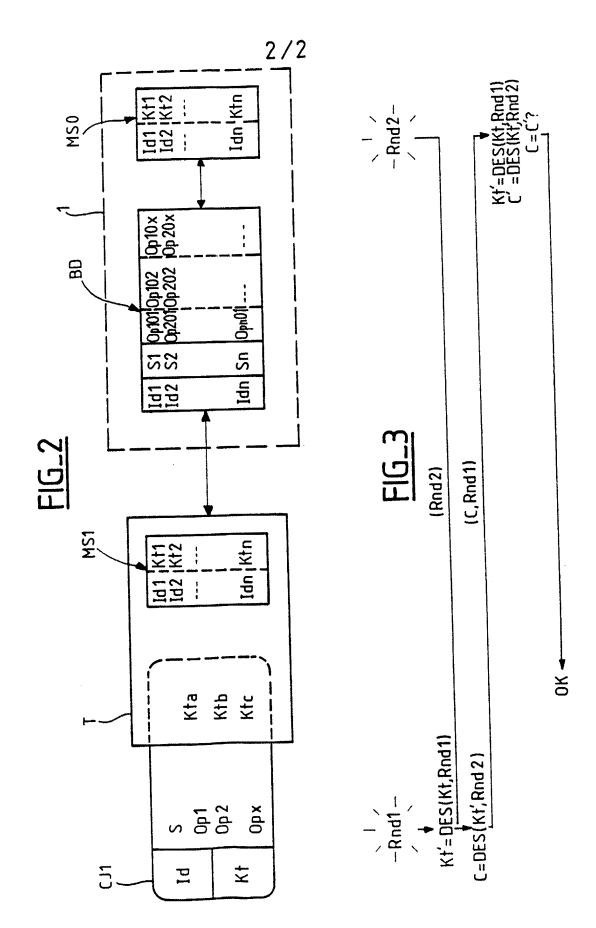
10

20

d'authentification (C') calculé par la carte de jeu ou par un autre module de sécurisation (MS1).

- 19. Système sécurisé selon la revendication 18, caractérisé en ce qu'un module de sécurisation (MS1) est disposé dans le transcripteur (T, 10, 210, 310).
- 20. Système sécurisé selon l'une des revendications 18 et 19, caractérisé en ce qu'un module de sécurisation (MSO) est disposé dans une machine de jeu (200).
- 21. Système sécurisé selon l'une des revendications 18 à 20, caractérisé en ce qu'un module de sécurisation est disposé sur les moyens de liaison du réseau.
- 22. Système sécurisé selon l'une des revendications 18 à 21, caractérisé en ce qu'un module de sécurisation (MSO) est disposé dans l'organe central de gestion (1).
- 23. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte à puce.
 - 24. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte sans contact.
 - 25. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte bancaire.





INTEL ATIONAL SEARCH REPORT

PCT/FR 98/00582

			PCT/FR 98/00582
A. CLASSII IPC 6	FICATION OF SUBJECT MATTER G07F17/32 G07F7/08		
According to	o International Patent Classification(IPC) or to both national classi	fication and IPC	
	SEARCHED		
Minimum do IPC 6	ocumentation searched (classification system followed by classific $607F$	ation symbols)	
Documentat	tion searched other than minimum documentation to the extent tha	at such documents are include	d in the fields searched
Electronic d	lata base consulted during the international search (name of data	base and, where practical, se	arch terms used)
C. DOCUM	ENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the	relevant passages	Relevant to claim No.
Υ	WO 93 17403 A (NSM) 2 September	1993	1-5,16, 23
	see abstract; claims 13-24; fig see page 6, paragraph 2 - page paragraph 1		
Y	DE 44 27 039 A (GIESECKE & DEVI February 1996 see abstract; claims; figures see column 3, line 32 - column	1-5,16, 23	
Α	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 March 1994 see abstract; claims; figure see column 4, line 8 - column		1-6,16, 23
Α	WO 96 08798 A (GEMPLUS) 21 Marssee abstract; claims; figures	ch 1996	1,2,6-23
X Fun	ther documents are listed in the continuation of box C.	Y Patent family m	embers are listed in annex.
° Special c. "A" docum consi "E" earlier filing "L" docum which citatic "O" docum other "P" docum later	nent defining the general state of the art which is not idered to be of particular relevance of document but published on or after the international date of the art which may throw doubts on priority claim(s) or his clted to establish the publicationdate of another on or other special reason (as specified) ment referring to an oral disclosure, use, exhibition or means on the published prior to the international filing date but than the priority date claimed	or priority date and cited to understand invention "X" document of particul cannot be consider involve an invention "Y" document of particul cannot be consider document is combinents, such combinents, such combinents, and coument member of the combinents." "&" document member of the combinents."	ished after the international filing date not in conflict with the application but at the principle or theory underlying the lar relevance; the claimed invention red novel or cannot be considered to e step when the document is taken alone lar relevance; the claimed invention red to involve an inventive step when the inventive step when the internation being obvious to a person skilled of the same patent family
	21 July 1998	31/07/19	998
Name and	d mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer	J

INTERNA JNAL SEARCH REPORT

Int. Ional Application No PCT/FR 98/00582

		PCT/FR 98/00582			
C.(Continue	ation) DOCUMENTS CONSIDERED TO BE RELEVANT				
Category °	Citation of document, with indication, where appropriate, of the relevant passages		Relevant to claim No.		
A	EP 0 762 333 A (TEXAS INSTRUMENTS) 12 March 1997				
A	EP 0 619 564 A (PITNEY BOWES) 12 October 1994				
A	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 January 1997				

INTERI MONAL SEARCH REPORT

information on patent family members

PCT/FR 98/00582

Patent document cited in search report		Publication date			atent family member(s)	Publication date
WO S	9317403	A	02-09-1993	DE AT DE EP US	4205791 A 132992 T 59301417 D 0628192 A 5557086 A	02-09-1993 15-01-1996 22-02-1996 14-12-1994 17-09-1996
DE 4	 4427039	 А	01-02-1996	EP	0696021 A	07-02-1996
EP (0589545	Α	30-03-1994	US AU AU CA	5371345 A 660561 B 4623393 A 2105925 A	06-12-1994 29-06-1995 24-03-1994 18-03-1994
WO	9608798	Α	21-03-1996	FR AU ZA	2724748 A 3475695 A 9507809 A	22-03-1996 29-03-1996 07-05-1996
EP	0762333	A	12-03-1997	JP	9297862 A	18-11-1997
EP	0619564	A	12-10-1994	US EP AT AU CA CA CA DE DE DE DE EP	4802218 A 0619563 A 0619565 A 116778 T 160456 T 160039 T 605443 B 7961287 A 1320578 A 1326911 A 1335839 A 1296809 A 3750958 T 3752138 D 3752138 T 3752146 D 3752146 T 228888 A 0294397 A 0740275 A	31-01-1989 12-10-1994 12-10-1994 15-01-1995 15-12-1997 15-11-1997 10-01-1991 24-03-1988 20-07-1993 08-02-1994 06-06-1995 03-03-1992 16-02-1995 08-06-1995 11-12-1997 26-03-1998 02-01-1998 09-04-1998 17-06-1988 14-12-1988 30-10-1996

INTERNA)NAL SEARCH REPORT

information on patent family members

Ints. sional Application No PCT/FR 98/00582

Patent document cited in search report		Publication date	Patent family member(s)		Publication date	
EP 0619564	A	<u> </u>	FI JP JP NO WO US US	882047 A,B, 1500863 T 2661932 B 300660 B 8801818 A 4864618 A 4900904 A 4900903 A	02-05-1988 23-03-1989 08-10-1997 30-06-1997 10-03-1988 05-09-1989 13-02-1990	
WO 9702547	A	23-01-1997	NL AU EP NO	1000741 C 6613096 A 0836730 A 976151 A	08-01-1997 05-02-1997 22-04-1998 03-03-1998	

RAPPORT DE R. .IERCHE INTERNATIONALE

Dec. de Internationale No PCT/FR 98/00582

A. CLASSEMENT DE L'OBJET DE LA DEMANDE CIB 6 G07F17/32 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 GO7F

Documentation consultée autre que la documentationminimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si celaest réalisable, termes de recherche utilisés)

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no, des revendications visées
Υ	WO 93 17403 A (NSM) 2 septembre 1993	1-5,16, 23
	voir abrégé; revendications 13-24; figures voir page 6, alinéa 2 - page 9, alinéa 1 	
Υ	DE 44 27 039 A (GIESECKE & DEVRIENT) 1 février 1996 voir abrégé; revendications; figures 1,2 voir colonne 3, ligne 32 - colonne 4, ligne 41	1-5,16,
Α	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) 30 mars 1994 voir abrégé; revendications; figure voir colonne 4, ligne 8 - colonne 8, ligne 56	1-6,16, 23

X Voir ia suite du cadre C pour la finde la liste des documents	X Les documents de familles de brevets sont indiqués en annexe
"A" document définissant l'état général de latechnique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date dedépôt international ou après cette date "L" document pouvant jeter un doute sur une revendation de	"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base del'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "T" document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme impliquant une activité inventive peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "8" document qui fait partie de la même famillede brevets
Date à laquelle la recherche internationale a étéeffectivement achevée 21 juillet 1998	Date d'expédition du présent rapport de recherche internationale 31/07/1998
Nom et adresse postale de l'administrationchargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk	
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

RAPPORT DE RE .ERCHE INTERNATIONALE De. de internationale No

De. de internationale No
PCT/FR 98/00582

	PC1/FR 98/00582		
OCUMENTS CONSIDERES COMME PERTINENTS	s pertinents no. des revendications visées		
identification des documents cités, avec, le cas échéant, l'indicationdes passages peru	noite no. u		
WO 96 08798 A (GEMPLUS) 21 mars 1996 voir abrégé; revendications; figures		1,2,6-23	
EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997			
EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994			
WO 97 02547 A (KONINKLIJKE PTT NEDERLAND) 23 janvier 1997			
	OCUMENTS CONSIDERES COMME PERTINENTS Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertium voir abrégé; revendications; figures EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997 EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994 WO 97 02547 A (KONINKLIJKE PTT NEDERLAND)	OCUMENTS CONSIDERES COMME PERTINENTS Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents NO 96 08798 A (GEMPLUS) 21 mars 1996 voir abrégé; revendications; figures EP 0 762 333 A (TEXAS INSTRUMENTS) 12 mars 1997 EP 0 619 564 A (PITNEY BOWES) 12 octobre 1994 NO 97 02547 A (KONINKLIJKE PTT NEDERLAND)	

RAPPORT DE L HERCHE INTERNATIONALE

Renseignements relatifs aux membres de families de brevets

PCT/FR 98/00582

Document brevet cité au rapport de recherche W0 9317403 A DE 4427039 A EP 0589545 A W0 9608798 A		е	Date de publication		nbre(s) de la e de brevet(s)	Date de publication
WO	9317403	Α	02-09-1993	DE AT DE EP US	4205791 A 132992 T 59301417 D 0628192 A 5557086 A	02-09-1993 15-01-1996 22-02-1996 14-12-1994 17-09-1996
DE	4427039	Α	01-02-1996	EP	0696021 A	07-02-1996
EP	0589545	Α	30-03-1994	US AU AU CA	5371345 A 660561 B 4623393 A 2105925 A	06-12-1994 29-06-1995 24-03-1994 18-03-1994
WO	9608798	Α	21-03-1996	FR AU ZA	2724748 A 3475695 A 9507809 A	22-03-1996 29-03-1996 07-05-1996
EP	0762333	А	12-03-1997	JP	9297862 A	18-11-1997
EP	0619564	A	12-10-1994	US EP EP AT AU CA CA CA DE DE DE DE DE DE EP	4802218 A 0619563 A 0619565 A 116778 T 160456 T 160039 T 605443 B 7961287 A 1320578 A 1320578 A 1326911 A 1335839 A 1296809 A 3750958 D 3750958 T 3752138 D 3752138 T 3752146 D 3752146 T 228888 A 0294397 A 0740275 A	31-01-1989 12-10-1994 12-10-1994 15-01-1995 15-12-1997 15-11-1997 10-01-1991 24-03-1988 20-07-1993 08-02-1994 06-06-1995 03-03-1992 16-02-1995 08-06-1995 11-12-1997 26-03-1998 02-01-1998 02-01-1998 03-04-1998 17-06-1988 14-12-1988 30-10-1996

RAPPORT DE RECI CHE INTERNATIONALE

Renseignements relatifs aux membres de families de brevets

De. de internationale No PCT/FR 98/00582

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0619564 A		FI 882047 A,B, JP 1500863 T JP 2661932 B NO 300660 B WO 8801818 A US 4864618 A US 4900904 A US 4900903 A	02-05-1988 23-03-1989 08-10-1997 30-06-1997 10-03-1988 05-09-1989 13-02-1990
WO 9702547 A	23-01-1997	NL 1000741 C AU 6613096 A EP 0836730 A NO 976151 A	08-01-1997 05-02-1997 22-04-1998 03-03-1998

Nº727 WO P. 2/323 PCT/FR98/00582

REÇU le

0 2 NOV. 1998

PCT

AVIS INFORMANT LE DEPOSANT DE LA

COMMUNICATION DE LA DEMANDE

INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT).

Expéditeur: le BUREAU INTERNATIONAL

Deszinataire:

NONNENMACHER, Bernard

Gemplus S.C.A.

Z.I. Athelia III Vaie Antiope

F-13705 La Clotat Cedex

or.

99 .

FRANCE

Date d'expédition (jour-mojs:année)

22 octobre 1998 (22.10.98)

Référence du dossier du déprésant ou du mandataire

GEM 362

Déposant

AVIS IMPORTANT

Date du dépût international (jour mois/année)

Date de priorité (jour/mojs/snnée)

Demands internationals no PCT/FR98/00582

20 mars 1998 (20.03.98)

11 avril 1997 (11.04.97)

GEMPLUS S.C.A. etc

1. Il est natifié par la présente qu'à la date indiquée di-dessus comme date d'expédition de cet avis, le Bureau international a communique, comme le prévoit l'arquée 20, la demange internationale aux offices désignée suivants:

AU, BR, CA, CN, EP, JP, KR, US

Conformément à la règle 17.1.c. troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communicazion de la cernande internationale a bien eu liau à la date d'expédition indiquée plus haut, et le du fait que la communicazion de la cernande internationale à l'office du aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être éffectuée à cette date:

MX,RU,SG,VN

La communication serà effectuée seulement sur demande de gas offices. De plus, le déposant n'est pas tonu de remettre de copie de la demande internationale aux affices en question (règle 49.1)a-bis)).

3. Le présent avis est accempagné d'une copie de la demande internationale publiée par le Bureau international le 22 octobre 1998 (22.10.98) sous le numéro WO 98.47113

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite recorter l'ouverture de la phase nationale jusqu'à 36 mois (ou plus pour ce qui concerné certains offices) à compter de la date de priorité, la demande d'exames préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de proprié.

Il appardent exclusivement au déposant de veiller au respect du délai de 19 mois. compter de la date de pronté.

Il est à noter que seul un déposem qui est ressortissem d'un État contractent du PCT llé par le chapitre il ou qui y a son domicile bent blessuter nue demande d'examen breilminaire international

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaire que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu-

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase restionale, voir l'annexe du formulaire PCT/B/301 (Notification de la récaption de l'exemplaire original) et le volume il de l'étable du décaption de Brit. du Guide du dénosant du PCT.

> Bureau international de l'OMPI 34, phemin des Colombettes 1211 Genève 20, Suisse

Fonctionnaire autorisé

J. Zahra

no de téléphone (41-22) 338.83.88







ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTURILE Bureau international

DEMANDE INTERNATIONALE FUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

DEMANDE INTERNATIONALE PUBLIEE EN VERT	U DU	TRAFFE DE COOFERATION EN MO 98/47113
(51) Classification internationale des brevets	AI	(11) Numéro de publication internationale: WO 98/4/113 (43) Date de publication internationale: 22 octobre 1998 (22,10.98)
G07F 17/32, 7/08		(43) Date de printestation 251 PP CA CN, IF, KR, MX, RU, SG, US.

PCT/FR98/00582 (21) Numéro de la demande internationale:

20 mars 1998 (20.03.98) (22) Date de dépôt interpational:

(30) Données relatives à la priorité: FR. 11 avril 1997 (11,04.97) 97/04733

(71) Déposant (pour tous les États désignés souf US): GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Besugue, Paus d'activités de Gémenos, F-13881 Gémenos Cedex (FR).

(75) Inventeurs/Hopesants (US seulement: ORUS, Hervé [FR/FR]; 20, rus de la Grafounie. Zac Lon Caire. F-13470 Carocus en Provence (FR). FOGLINO, Sem-Seques [FR/FR]; Les Terrasses de l'Audiguler, F-19790 Peyrier (FR).

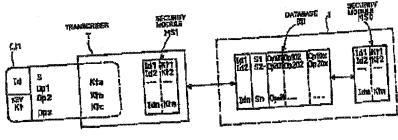
(74) Mandataire: NONNENMACHER, Bernard; Gempius S.C.A. ZI Athelia III, Vois Antiope, F-15705 La Cione Cedex

(81) Etats désignés: AU, BR, CA, CN, IP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publice

Avec rapport de recherche internationale.

- SECURITY PROCEDURE FOR CONTROLLING THE TRANSFER OF VALUE UNITS IN A CHIP CARD GAMING (54) Title:
- (54) Tide: PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTÈME DE IEU A CARTES A PUCE



OP ACTORN PLANEY

The invention concerns slot machines, such as jackpot or black jack and other casino gumbling machines. The machines are designed (57) Abstract the invention concerns sur manner, such as pacapet or easier jack and course manner manner manner manner unit (1). The invention is to operate with gaming cants (CII), such as this cants, and are connected by network to a control management unit (1). The invention is to operate with gaping cases (C11), such as this cases, and are connected by network to a control management unit (1). The investion is characterised in that the crutial management unit comprises a database (ED), wherein are stored data corresponding to those stund on the gaming cards such data concerning the account balance stored in the card data concerning the gamester and card identification data (Id) and data (S, Op1, Op2) concerning the account balance stored in the card (CII). The procedure consists in verifying the card data with respect to the control management unit database to ensure the integrity of such a gambling machine system operating with thin cands or contactless cands.

DE

Themendads.

LR LR

Sri Lanks





L'invention concernt les machines à sons, type jack-pot, black-jack, et autres machines de jeu d'argent de casino. Il est prévu que les machines de jeu fopetionnent avec des cames de jeu (CII), type caste à price, et sont relifées en réseau avec un organe central de gestion (CII). L'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont anockées des informations de l'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont avec des central de gestion comporte une base de données (BD) de des después (BD) de l'invention prévoit que l'organe central de gestion comporte une base de données (BD) de des después (BD) de l'invention prévoit que l'organe central de gestion de l'invention prévoit que l'organe central de gestion de l'invention de l'in (1). L'invention prevoit que l'organe central de gestion comporte une pase de dounées (BD), quis saquette sont stockées det informations sur le joueur ainsi que des données (Id) d'identification des comespondantes à celles stockées sur les cautes de jeu comme des informations sur le joueur ainsi que des données (Id) d'identification des cautes et des données (S, Opl., Op2) renseignant sur le splide de la valeur stockée dans la caute (CII). Une vérification des données de la caute par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des causes à puct on des caries sans contact.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Eurs parties au PCT, sur les pages de converture des brochures publiant des demandes internationales en verm du PCT.

al am at	Allumia Anniche Anniche	ES TA TA GA	Espagai Francis Francis Gallon	ra In Il	Lesonic Liggenic Lesonic Materia	si sk sn sz td	Slovénie Slovagnie Sénégal Bouzziand Tehad
AU AZ BA BA ES BE BY BG BI ER CA CF CG CG CG CG CG	Anadralic Anadralica Anadralica Bosolo-Berralgovipa Barbala Barbala Belgingo Bosolo Belgingo Belgingo Belgingo Belgingo Castala Répoblique cantalification Congre Eules d'insine Cantala	GE G	Regamme Upit Géorgie Grouta Grinde Grèce Hongrie frinade lepail Edware Injue Lapan Kanya K	MC MG	Régultique de Moldava Mutagraces Ex-Régultique yougosisyo de Maccidaine Malli Mongolie Mantanie Mantanie Mantanie Mantanie Mantanie Maryi Maccidae Migur Raya-Bas Maryi-Bas Monyelle-Zélando Pologre Horogal Boarsanie	To Tim Tra Ita Ua UG UZ VN YII Zw	Togo Tudijkintan Tuskintan Tuskint Tuskint Tuskint Tuskint Onganda Ball-Unis d'Amériqua Onubekintan Vest Sam Yengadavio Zimbalres
CN CN CZ	Chine Cuba République mièque: Allemakue	EZ LC LJ	Karakatan Sainer-Lucib Licenseptein	D SD SR	Redécusion de Russie Sandan Suede		

Singspoor



5

10

15

20

25

30

PCT/FR98/00582

NQ727

PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU À CARTE À PUCE

Le présente invention concerne le domaine des machines à sous, telles que les dispositifs de jack-pot et les autres dispositifs de jeux d'argent individuels du type de ceux que l'on trouve dans les casinos.

Elle concerne plus particulièrement des machines à sous permertant d'enregistrer des mises et des gains avec des cartes de jeu. Les cartes de jeu sont du type carte à puce cu carte sans contact. Les cartes de jeu peuvent être dédiées à catte utilisation suivant cartas táléphoniques. Elles l'exemple des avantageusement constituées par des cartes bancaires, d'argent sommes permettant de transférer des directement sur la machine à sous.

La présente demande vise un procédé et un système de contrôle de transfert d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines jeu, chaque machine étant connectée transcripteur de données sur cartes de jeu apte à créditer et/ou à débiter des unités de valeur en mémoire d'une carte de jeu.

Un objectif général du contrôle de transfert d'unités de valeurs entre cartes de jeu et machines de jeu est d'évitar toute malversation financière à l'aide de telle cartes.

on connaît déjà des systèmes de gestion pour des machines de jeu équipées de lecteurs de cartes à puce, adaptés à la gestion d'un parc de machines de jeux sites relativement fermés et disposées dans des contrôlés comme les casinos. Ces systèmes sont adaptés à un tel environnement, car il font l'objet de de réglementations importants, peu contrâles et

5

ŢŎ

. 72

20

25

QE



susceptibles de permettre des fraudes sur les transactions de jeux utilisant des cartes à puce.

Le document EP-A-O 360 613 décrit par exemple un système de transfert de données entre carte à puce et une pluralité de machines avec des moyens de transmission et de stockage des données machine dans la carte à puce. Un tel système parmet d'effectuer un carte à puce. Un tel système parmet d'effectuer un relavé des opérations de jeu avec une carte de collecte stockant une liste des opérations de jeux effectuées dans un but comptable ou fiscal.

Un inconvénient d'un tel système est qu'on ne peut pas contrôler toutes les opérations de jeu effectuées, sauf à relever toutes les machines avec la carte de collecte, ce qui occasionne des manipulations fastidieuses.

D'autre part, devant la demande croissante du public, il est envisagé d'installer des machines de jeu dans des sites moins protègés que les casinos comme des salles de jeux privées ou des bars, voire même dans des lieux d'habitation privés comme le domicile des joueurs.

joueurs.

Il apparaît clairement qu'une telle dispersion des machines de jeu pose d'importants problèmes de sécurité des transactions suite aux opérations de jeu.

Un but de l'invention est de permettre un développement des machines de jeu fonctionnant avec des cartes à puce dans des lieux non protégés.

Un autre but de l'invention est de renforcer l'intégrité des systèmes de machines de jeux fonctionnant avec des cartes de jeu.

L'invention prévoit que les machines de jeu sont reliées en réseau avec un organe central de gestion. Selon l'invention on a prévu que l'organe central de gestion comporte une base de données, dans laquelle

ã

10

15

20

ż

PCT/FR98/00582

sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur zinsi que des données d'identification des cartes et des données renseignant sur le solde de la valeur stockée dans la carte. Une vérification des données de la carte par rapport aux données de la base l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans

L'invention prévoit ainsi un procédé sécurisé de contact. contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines chaque machine étant transcripteur de données sur carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :

- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification de la carte et des données représentatives des unités de valeur débitées et/ou créditées au cours des opérations précédentes,
- échanger des Connées entre la machine et une base données de l'organe central de gestion 25 du rěseau l'intermédiaire des moyens de liaison sécurisé, notamment des données représentatives de valeur et/ou solde des unités de d'identification de la carte ; et, 30
 - vérifier que les données en mémoire de la carte de jeu correspondent aux données de la base de données afin de contrôler l'intégrité d'un système constitué

5

10

15

20

25

30

PCT/FR98/00582

Nº727

par une telle carte, une telle machine, le réseau et l'organe central de gestion.

L'invention prévoit avantageusement des moyens de sécurisation qui permettent d'authentifier les messages de données échangées sur le réseau, c'est-à-dire de signer de tels messages.

L'invention prévoit en outre un système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apta à débiter des unités de valeur d'une carte de jeu, les machines étent reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, une carte de jeu stockant en mémoire des données représentatives d'opérations de jeu effectuées, notamment des données d'identification de la carte et des données regrésentatives de solde des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de données une base de gestion comporte parallèlement en mémoire les données représentatives des opérations de jeu effectuées, notamment les données et cartes d'identification représentatives des soldes des valeurs débitées et/ou des créditées au cours des cpérations de jeu précédentes et en ce que des moyens de contrôle vérifient que, pour une carte identifiée, les données de la base et les données de la carte correspondent, notamment que les données représentatives du solde correspondent, afin de vérifier l'intégrité du système.

Un module de sécurisation pour l'authentification des messages de données peut avantageusement être prévu dans le réseau, au niveau d'un transcripteur, d'une

5

10

15

20

25

30

PCT/FR98/00582

machine, de l'organe central, ou même des moyens de liaison du réseau.

L'invention sera mieux comprise à la lecture de la qui suivent, donnés description et des dessins uniquement à titre d'exemples non limitatifs ; sur les dessins annexés :

- la figure 1 représente un système sécurisé de contrôle de transfert d'unités de valeurs entre une pluralité de cartes de jeu et une pluralité de machines de jeu apre à mettre en oeuvre l'invention ;
- la figure 2 représente un schéma d'échange et de vérification des données selon l'invention ; et,
- la figure 3 représents un calcul de certificat d'authentification par des moyens de sécurisation salon l'invention.

sur la figure 1 on a représenté un système sécurisé de machines de jeu tel que proposé par l'invention, et qui comprend une ou plusieurs machines de jeu 200, 200', 200" et 200'".

Une telle machine de jeu 200, semblable aux machines à sous que l'on trouve dans les casinos dispose d'un monnayeur électronique 210 que l'on appellera par la suite transcripteur de données sur

Le transcripteur de données sur carte 210 est relié carte de jeu CJ. à l'électronique de la machine 200, par exemple par une liaison série de type RS 485. La machine et le lecteur comportent des interfaces entrée-sortie adaptées à cette liaison.

De façon classique, la machine est équipée d'un écran d'affichage 211 qui permet aux joueurs de savoir à tout instant quel est le solde dont il dispose pour jouer et le montant des mises et des gains réalisés.

5

IO

Įā

20

25

30





PCT/FR98/00582

ă

La machine 200 qui a été représentée peut bien sur <u>électronique</u> monnayeur machine à. à double me être machine mais aussi une monnayeur, c'est-à-dire une machine qui comporte outre ce monnayeur électronique, un monnayeur à pièces (ou à jetons) symbolisé par la ráférence 201.

Dans le cas d'une machine à double monnayeur, le joueur aura la possibilité de jouer avec des pièces ou jetons et de se faire restituer ses gains uniquement sous la forme de pièces.

les certes de jeu CJ représentées sous forme de cartes à puce comportent une mémoire morte effaçable électriquement, par exemple une mémoire de type EFPROM.

Il peut s'agir également de cartes mémoira comportant un microprocesseur, une programmes et une mémoire de travail de type RAM.

Ces cartes à puce peuvent également être des cartes à chargement d'unités de type rechargeable. Ces cartes comportent pour cela une mémoire électriquement programmable du genre boulier.

En outre les cartes de jeu peuvent être constituées par des cartes sans contact, la carte comportant un circuit intégré à mémoire et microprocesseur, et un circuit électronique de transmission de données sans contact électrique. On peut par exemple utiliser un transpondeur tel que décrit dans la demande de brevet FR - 96 16061.

La réalisation des machines de jeu 200 et leur connexion à des transcripteurs de données sur cartes de jeu ne sera pas détaillée ici. Des exemples réalisations de machines de jeu sont détaillés par exemple dans la demande de brevet FR - 96 10031 dont la description est incorporée à la présente.

10

15

20

25

aa

.1161

WO 98/47113

7

Afin de contrôler les opérations de jeux et les transactions avec les cartes, il est prévu de relier les machines 200, 200', 200", 200'" en réseau, avec un organe central de gestion représentés sous la référence 1 à la figure 1. Les machines du réseau sont reliées à l'organe central de gestion 1 par des moyens de liaison 123. Comme représentées à la figure 1, les machines 200, 200', 200", 200'" peuvent également être reliées entre elles par le réseau.

Les moyens de liaison 123 sont constitués dans le cas d'un réseau local comme calui d'un casino par une liaison locale. La liaison locale est par exemple une liaison série de type RS 485, un bus de liaison parallèle , une fibre optique, une liaison radio ou tout autre support de transmission.

Dans le cas d'un réseau joignant des salles de jeu les poyens de liaisons peuvent être constitués par des canaux de transmission propres au réseau ou par des lignes téléphoniques.

Pour établir des liaisons téléphoniques, le réseau comporte des modulateurs-démodulateurs de type MODEM 120, 120', 120" et 120"', disposés en interface entre les moyens de liaison 123 et une machine de jeux 200, 200', 200", 200"' respectivement.

L'organe central de gestion l'est constitué par exemple d'un ordinateur central relié également aux moyens de liaison 123 par un MODEM 101 de façon à faire partie du réseau.

Sur la figure 1 on a représenté des moyens de liaison 123 sous la forme schématique d'une ligne annulaire à laquelle les machines de jeux 200, 200', 200" et 200"! sont connectées. Les machines sont ainsi reliées entre elles et à l'organe central de gestion 1.

5

10

15

20

25

30

La liaison peut cependant prendre toutes sortes de formes équivalentes.

Dans le cas de liaisons téléphoniques, les machines sont reliées individuellement aux moyens centralisés de pas nēcessairement les machines n'étant reliées entre elles. Le MODEM 101 des moyens de gestion peut comporter avantageusement un standard plusieurs lignes téléphoniques.

L'utilisation de liaisons téléphoniques présente l'avantage de permettre d'étendre le réseau au lieu d'habitation des joueurs. Les machines de jeux sont de préférence constituées par des ordinateurs personnels 300 et 300' de type PC. Les machines peuvent ainsi être connectées chacune à un transcripteur de données sur carte de jeu 310 cu 310' intégrant de préférence un MCDEM 130 on 130', par exemple du type commercialisé par la demanderesse.

Le réseau utilisé peut être notamment un réseau de communication ouvert du type "INTERNET".

Il est prévu en outre que le système et le réseau terminal de moins un reprêsenté à la figure 1 sous forme d'une caisse enregistreuse 100. Le terminal de chargement comporte alors un transcripteur 110. Le terminal 100 et le transcripteur 110 sont alors reliés au réseau par l'intermédiaire d'un MODEM 111 connecté aux moyens de

Classiquement, il est prévu que les cartes à puce liaison 123. dédiées aux jeux sont des cartes non-rechargeables, à l'instar des cartes téléphoniques, et elles sont fabriquées et chargées uniquement par un organisme

avec des cartes central. application rechargeables, il est prévu que la base de données BD

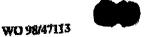
10

15

20

25

3 O



des moyens centralisés de gestion l dispose des soldes S1, S2, ..., Sn initiaux des valeurs créditées sur les cartes CJ1, CJ2, ..., CJn avant

Capendant, salon une variante avantageuse, il est circulation. prévu que les cartes sont rechargées en unités de valeurs par l'intermédiaire de terminaux de chargement.

En pratique, ce terminal peut être celui d'un caissier du casino. De façon alternative, on peut prévoir une multitude de terminaux de chargements disposés dans des débits de tabac ou dans d'autres commerces accessibles aux joueurs.

Ainsi lorsqu'un joueur désire obtenir la délivrance d'un crédit, il donne sa carte de jeu CJI à l'opérateur habilité à utiliser le terminal 100 qui însère cette carte dans la partie transcripteur 110 de ce terminal 100 et qui au acyen du clavier de la caisse va rentrer le montant du crédit que désire avoir le joueur. Ce montant est transféré eu transcripteur 110 qui enregistre alors sur la carta à puce CJI l'information significative correspondant au crédit désiré par le

Selon l'invention, le terminal de rechargement peut joueur. alors communiquer à l'organe central de gestion 1, par l'intermédiaire des moyens de liaison du réseau 123, les données lues sur la carte à recharger, notamment son numéro d'identification Id et son solde S d'unités de valeur. La vérification du numéro d'identification Id de la carte de jeu CJ1 peut être faite directement par le terminal de rechargement 100 ou par son transcripteur de données 110 ou de manière alternative par l'organe central de gestion 1. L'invention prévoit ainsi une étape préliminaire aux opérations de jeu, consistant à inscrire dans la base de données de

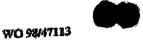
10

1.5

20

25

30





10

PCT/FR98/00582

l'organe central de gestion l et dans la mémoire d'une carte de jeu CJI, des données représentatives d'une d'une lors solde initial de valeur préliminaire de chargement de la carte CJI.

Selon la première alternative, il est prévu comme visible à la figure 2 que le terminal de rechargement dispose transcripteur T d'identification secrètes Kt1, Kt2, ..., Ktn de toutes les cartes de jeu CT1, CT2, ..., CJn en circulation. Ces clès secrètes sont de préférence stockées dans un module de sécurisation MSI comportant une mémoire et une unité de calcul, les données stockées n'étant pas accessibles de l'extérieur. Le terminal 100 vérifie alors que l'identification Id1 de la carte à puce CJ1 est correcte avec la clef Ktl correspondante, appliquant un algorithme d'authentification ou de cryptage selon les méthodes connues.

alternative, seconde authentification de la carte est effectuée au niveau de 1, gestion l'organe central de clefs les Id1, Id2, ..., Idn et d'identification d'authentification correspondantes Kt1, Kt2, ..., Ktn étant stockées dans la base de données BD de l'organe central de gestion ou de préférence dans un module de sécurité MSD similaire à MSI. Cette seconde alternative présente l'avantage d'éviter toute dissémination des clefs d'authentification secrêtes.

L'invention prévoit en outre un échange de données entre le terminal et l'organe central de gestion portant sur les données stockées dans la base de gestion l'organe central de préférence, cet échange de données est accompagné d'un protocole d'authentification. ប្រា sécurisation permettant d'émettre de tels certificats

WO 98/47113

5

10

15

20

25

30



PCT/FR98/00582

protocole ci-aprēs. Ce détaillé avantageusement qu'une machine parasite du réseau ne crédite abusivement la base de donnée. Le terminal T peut ainsi communiquer le solde S des valeurs débitées at/ou créditées précédemment sur la carte de jeu CJ1 à l'organe central de gestion 1. Après avoir authentifié le numéro d'identification Idl de la carte ou le certificat accompagnant les données de solde, on peut ainsi vérifier que le solde S inscrit en mémoire de la carte de jeu CJI correspond bien au solde S1 stocké dans la base de données BD. Si la vérification est positive, il est prévu que l'organe central de gestion 1 émet un signal d'accord pour le rechargement de la carta CJL par le terminal et le transcripteur T. En cas de vérification négative, une procédure ou un signal . d'alerte peuvent être mis en ceuvre au niveau de l'organe central de gestion I, ou au niveau du terminal de chargement. Dans un réseau de machines à sous de casino par exemple, le caissier pourra être alerté par le terminal de chargement afin de découvrir l'origine d'un tel dysfonctionnement. Dans un réseau plus étendu, on peut prévoir que la carte CJ1 soit avalée par le transcripteur T du terminal afin d'enquêter sur le dysfonctionnement.

On peut prévoir en outre que la base de données ou la mémoire des cartes de jeu CI comportent des informations sur le joueur, par exemple sur son âge, applications jeu pour des habitudes de parties remise de joueurs, de fidelisation des gratuites, etc.

Nous allons présenter maintenant des protocoles de contrôle de transferts d'unités de valeur au cours d'opérations de jeu effectuées avec le procédé ou le système selon l'invention.

5

10

15

20

25

30

ı



PCT/FR98/00582

Au début des opérations de jeu, le transcripteur de données sur carte 210 de la machine de jeu lit le numéro d'identification en mémoire de la carte de jeu CII. Comme exposé précédemment au vu de la figure 2, ce préférence est. d'identification Id authentifié par un module de sécurité MS1 prévu dans le transcripteur T. Le numéro Id peut éventuellement être communiqué à l'organe central de gestion 1 en vue CJI carta d'authentifier <u>1</u>a dans le module d'identification Wil contenue sécurité MSC. Catte étape d'identification est de préférence effectuée une seule fois pour plusieurs opérations de jeu avec la même carte sur la même le terminal mémorisant machine ou éventuellement ce numéro d'identification Id pour les

12

cpérations suivantes.

A chaque opération de jeu suivante, le solde S des unités de valeur affecté au joueur est revu à la suite des mises ou des gains réalisés.

gelon un pramier mode de réalisation de selon un pramier mode de communiquer simplement à l'invention, il est prévu de communiquer simplement à l'organe central de gestion 1 des données relatives à l'organe central de jeu effectuée, notamment le nouveau solde d'unités de valeur obtenu au cours de cette opération de jeu. L'organe central de gestion 1 peut opération de jeu. L'organe central de gestion 1 peut ensais stocker la liste des opérations effectuées, sous forme d'une liste des crédits ou des débits successifs enregistrés sur la carte CJI. Cette liste des opérations Oplo1,Oplo2,..., Oplox est par exemple opérations Oplo1,Oplo2,..., Oplox est par exemple enregistrée dans la base de données BD sous le numéro d'identification Id1 de la carte CJI en cours d'identification Id1 de la carte CJI en cours

d'utilisation. La recopie du solde S1 ou des opérations Opi01, Opi02, ..., Opi0x dans la base de données BD de

P. 17/32

WO 98/47113

5

10

15

20

25

30

l'organe central de gestion 1 sert alors à établir un relevé comptable des opérations ou à effectuer des un tel várifications fiscales. opérations permet également lors d'une vérification d'une carte falsifiée de mesurer l'étendue de la

réalisation de fraude. de mode deuxième l'invention, il est prévu une étape supplémentaire consistant à vérifier que les données en mémoire de la carte CJI et les données de la base de données BD correspondent afin de contrôler l'intégrité d'un système constitué par une talle carte CJ1, une telle machine 200, le réseau 123 et l'organe central de

Deux types de vérification peuvent être prévues, la gestion L. numéro sur porter rouvant d'identification Id ou sur la solde S de la carte. vérification

La vérification du numéro d'identification Id1 de avec effectuée carte CII est d'identification Ktl comme on l'a vu précédemment. Selon ce deuxième mode de réalisation, le numéro d'identification Id est communiqué à l'organe central 1 via les moyens de liaison 123 du réseau. L'organe central 1 stocke les clés d'identification Ktl, Kt2, ..., Ktm des cartes CJ1, CJ2, ..., CJn en circulation, dans sa base de donnée BD ou de préférence dans un module de sécurisation MSO. Le module de sécurisation MSO effectue ainsi les calculs d'identification en

De plus, la vérification peut porter sur le solde interne. d'unités de valeur de la carte CJI. Dans ce cas, le transcripteur T lit sur la carte les données de solde S des unités de valeur et les envoie à l'organe central de gestion 1 par l'intermédiaire des moyens de liaison

5

10

15

20

25

30

14



du réseau 123. La vérification du solde S de la carte CJ1 est alors effectuée par rapport au solde S1 indiqué **ಷ**೦೩5 BD dannées đе d'identification Id1. Si les deux soldes S et S1 la base correspondent, l'opération de jeu est autorisée par l'organe central de gestion 1.

Selon une autre alternative, la vérification peut porter sur la certification des données échangées à Des algorithmes partir de la carte de jeu CJ1. standards d'encryptage de données type algorithme DES permettant en effet de certifier les données numériques échangées entre la carte CJ1, le transcripteur T, la machine de jeu et l'organe central de gestion 1. Le cryptage et le décryptage du certificat accompagnant les données transmises n'est possible et cohérent que si on utilise une clé secrète.

Les algorithmes de cryptage de donnés de type DES comportent des sáries de calculs complexes qui ne seront pas détaillés dans la présente.

Un exemple de mise en ceuvre d'algorithme DES sera en considérant simplement que l'algorithme fournit un nombre crypté, appelé clef de session K', à appelé premier nombre donné, d'identification K et d'un nombre aléatoire Rnd, selon partir d'un l'exemple de la formule suivante :

K' = DES(K, And)

La complexité des algorithmes DES rend impossible la découverte d'une clef d'identification secrète K à partir de la clef de session K' et du nombre aléatoire Rnd.

La figure 3 montre un exemple d'application d'un algorithme DES. Il permet d'illustrer des moyens de sécurisation du réseau, en particulier la sécurisation

5

10

15

20

25

30

15

des échanges de données effectuées via les moyens de liaison du réseau. La carte de jeu dispose dans une moins une zone mémoire inaccessible d'au d'identification secrète Kt. Le microprocesseur de la carte génère un nombre pseudo aléatoire Rndl. A partir de ces deux nombres Rndl et Kt, l'algorithme DES mis en oeuvre par le microprocesseur calcule une clef de session Kt'.

Cette clef de session Kt' peut servir de certificat d'authentification et être envoyée avec le nombre aléatoire Rnd1 et les données à certifier. Cependant, pour rendre toute découverte des clafs impossible, il est prévu d'appliquer une seconde fois l'algorithme DES. Comme visible figure 1, la carte de jeu, organe émetteur du message à certifier, demande à l'organe destinataire, l'organe central 1 par exemple, de lui fournir un second nombre aléatoire Rnd2.

L'algorithme DES est à nouveau appliqué à la clef de session Xt' et au second nombre aléatoire Rnd2 par le microprocesseur de la carte pour calculer un

Le message de données est alors envoyé à l'organe certificat C. descinataire accompagné du certificat C et du nombre aléatoire Rndl calculés par la carte. Ainsi les clefs utilisées, en particulier la clef d'identification secrète Kt, ne sont pas échangées.

du message de données L'authentification effectué en recalculant un certificat C' à partir des même données. L'organe central de gestion 1 dispose de sécurisé MSO madule d'identification secrête Kt. Le module sécurisé MSO peut donc calculer la clef de session Kt' à partir de la clef d'identification Kt et du nombre aléatoire Rndl.

ã

10

15

20

25

ЭO

9

WO 98/47113

PCI/FR98/00582

Le module sécurisé MSO dispose encore du nombre aléatoire Rnd2 qu'il a fourni précédemment à la carte de jeu. A partir de ces deux nombres Rnd2 et Kt', le module de sécurité MSO calcule à nouveau un certificat C' en appliquant une seconde fois l'algorithme DES.

16

En vérifiant que le certificat C calculé par la carte correspond au certificat C' recalculé par son module de sécurité, l'organe central peut authentifier le message de donnée reçu.

Notons que la clé de session Kt' et le certificat C sont recalculés à chaque certification de message désirée. On évite ainsi que une machine pirate du réseau obtienne l'accès à la base de donnée ou à la mémoire de la carte en recopiant une certification précédente.

Après avoir effectué une ou plusieurs de ces vérifications, l'organe central 1 envoie un signal d'accord qui peut être crypté ou encodé. Avec un tel signal d'accord, le joueur peut utiliser sa carte de jeu CIL, effectuer des mises, des opérations de jeu et racharger sa carte avec ses gains.

Dans ces deux premiers modes de réalisation, on a vu que la carte a une fonction d'identification, son numéro Id permettant à l'organe central 1 ou à la machine de jeu de la reconnaître voire de reconnaître le joueur dans certaines applications de fidélisation de clientèle. De plus, la carte a une fonction de perte-monnaie, le solde d'unités de valeur étant stocké perte-monnaie, le solde d'unités de valeur at la carte, la recopie de solde dans l'organe central 1 servant aux fins de vérification.

fins de verillos.

Selon un troisième mode de réalisation, la selon un troisième mode de réalisation, la fonction porte-monnaie n'est plus assurée par la carte pais par l'organe central de gestion lui-même. La carte pais par l'organe central de gestion lui-même.

WO 98/47113

5

10

lä.

20

25

30

17

ne comporte alors aucune donnée relative au solde du joueur mais uniquement des données d'identification, telles que le numéro d'identification Id, plusieurs Ktc d'authentification Kta, Ktb. éventuellement des informations sur le joueur. Les données de solde S1 des unités de valeur sont alors uniquement stockées dans la base de données BD de l'organe central de gestion 1. Ca compte d'unités de valeur se trouve par exemple dans la base de données sous le numéro d'identification Idl. 10

jeu, d'une cpération de d'identification Ii de la carte CJI est envoyé à l'organe central de gestion i via les moyens de liaison 123 du réseau. Le numéro d'identification Id peut être envoyé directement par la machine de jeu 200 ou par son transcripteur 210 s'il a été mémorisé par la machine ou par son transcripteur. Le numéro d'identification Id peut aussi âtre lu sur la carte et envoyé à l'organe central de gestion 1 par le transcripteur 210 à chaque

Après vérification du numéro d'identification Id, opération de jeu. l'organe central de gestion 1 consulte la base de données 3D et envoie à la machine de jeu 200 le solde S1 des unités de valeur affecté à la carte CJ1.

De préférence le transfert des données de solde d'unités de valeur est effectué avec un certificat selon le protocole de sécurisation des échanges de données présenté précédenment.

Un avantage de ce troisième mode de réalisation est que les montants mis en jeu sont stockés dans l'organe central de gestion 1, ce qui évite toute mémorisation de valeur au niveau des cartes de jeu.

Selon ce troisième mode de réalisation, il est donc prévu de stocker, dans la base de données des

10

15

20

25

02

WO 98/47113

PCT/FR98/00582

données les gestion, centralisés de représentatives du solde des valeurs débitées et/ou créditées afin d'éviter une fraude à partir d'une carte

18

Le contrôle consiste simplement dans ce troisième à puce. vérifier réalisation ā d'identification Id de la carte de jeu CJ1 avec une clé d'identification Ktl lue dans la base de données BD de l'orçane central de gestion 1 afin de contrôler l'intégrité de la carte.

Avec ces trois modes de réalisation de l'invention vu qu'on peut avantageusement contrôler l'intégrité des cartes de jeu utilisées sur les machines de jeu.

De glus, en mettant en ceuvre des moyens de sécurisation des échanges de données, l'invention permet avantageusement de vérifier l'intégrité d'un système formé par les cartes de jeu, le réseau de machines de jeu et la base de données de l'organe central de gestion, l'intégrité d'un des trois éléments du système, soit une carte de jeu, soit le réseau, soit la base de données étant vérifiée à l'aide des deux

L'invention prévoit en effet un système apte à autres éléments. mettre en ceuvre le procédé selon l'invention.

Un tel système comports une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apre à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau avec un organe central de gestion par l'intermédiaire de moyens de

Selon l'invention, les données représentatives des liaisonopérations de jeu effectuées avec une carte à puce sur une machine de jeu sont stockées en mémoire de la carte

10

15

20

25

30

1

de jeu et parallelement dans une base de données prévue dans l'organe central de gestion.

Les données stockées sont notamment les données d'identification de la carte et le solde ou les soldes successifs d'unités de valeur débitées et/ou créditées avec la carte.

Des moyens de contrôle tels qu'un programme d'ordinateur effectuant l'authentification du numéro d'identification de la carte ou la comparaison des valeurs de solde stockées sur la carte et dans la base ou encore la certification des données échangées sont pravus afin de vérifier l'intégrité du système.

De préférence, pour sécuriser les échanges de données sur le réseau, il est prévu qu'un module de sécurisation calcule un certificat d'authentification à partir de connées secrètes stockées en mémoire du module et en ce que les moyens de contrôle vérifient que le certificet d'authentification calculé par le certificat sécurisation correspond au d'authentification calculé par la carte de jeu ou par un autre module de sécurisation.

De tels modules de sécurisation MSO, MSI peuvent être disposés dans les cartes du jeu CJ1, CJ2, ..., CJn, cu au niveau des transcripteurs 10, 110, 210, 210', 210'', 210''', 310, des machines de jeu 200, 200', 200'', 200''', de l'organe central de gestion 1 ou même sur les moyens de liaison 123 du réseau.

On peut en particulier prévoir plusieurs modules ou des moyens répartis de sécurisation au sein du réseau. Chaque transcripteur 10, 210, 210', 210', 210"', ou chaque interface 11, 120, 120', 120", 120" comprend par exemple un module de sécurisation de sorte que les échanges de données sur les moyens de liaison 123 son accompagnés de "certificat d'authentification.

WO 98/47113

PCT/FR98/00582

Par exemple le transcripteur 10 émetteur ajoute à son message son certificat qui est authentifié par le transcripteur 210 destinataire avant d'être transmis à la machine 200 correspondante.

20

D'autres variantes de réalisation, avantages et caractéristiques de l'invention, apparaîtront à l'homme du métier sans sortir du cadre des revendications ciaprès.

10

15

30

WO 98/47113

PCT/FR98/00582

REVENDICATIONS

- contrôle de transferts de sécurisé d'unités de valeur entre une pluralité de cartes de jeu (CJ, CJ1, CJ2, CJn) et une pluralité de machines de jeu (200, 200', 200", 200''', 300, 300', 300"), chaque machine étant connectée à un transcripteur (210) de données sur carte de jeu (CJ2), les machines étant reliées en réseau sécurisé avec un organe central de çestion (1) par l'intermédiaire de moyens de liaison (123), le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :
 - lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification (Id) de la carte et/ou des données (5, représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes, le procédé étant caractérisé en ce qu'il comporte des êtapes consistant à :
- échanger des données entre la machine (200) et une base de données (BD) de l'organe central de gestion 20 (1) par l'intermédiaire des moyens de liaison (123) du réseau sécurisé, notamment des données représentatives de solde (5) des unités de valeur et/ou le numéro d'identification (Id) de la carte ; et, 25
 - vérifier que les données en mémoire de la carte de jeu (CJI) correspondent aux données de la base de données (BD) afin de contrôler l'intégrité d'un système constitué par une telle carte, une telle machine, le réseau et l'organe central de gestion.
 - 2. Procédé selon la revendication 1, caractérisé par étape préliminaire aux opérations de consistant à :



WO 98/47113

5

15

25

30

- inscrire, dans la base de données (BD) de l'organe central de gestion (1) et dans la mémoire d'une carte de jeu (CJI), des données représentatives d'un solde (S, Sl) initial d'unités de valeur lors d'une opération préliminaire de chargement de la carte.
- revendications áes l'une salon précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :
- inscrire, dans le base de données (BD) de données gestion (1), des l'organe central de représentatives du solde (S1) des unités de valeur de 10 la carte de jeu (CJ1). revendications
 - des l'une selon précédentes, caractérisé par une étape consistant, au Procédé cours d'une opération de jeu, à :
 - recevoir les connées représentatives du solde (S1) des unités de valeur à partir de l'organe central de gestion (1) afin d'éviter une fraude à partir d'une carte (CJ2) ou d'une machine de jeu (200).
 - des revendications <u>j</u>'une selon Procédé l'étape ce dae 20 précédentes, caractérisé en vérification consiste à :
 - vérifier les données représentatives de solde (S) des unités de valeur lues en mémoire de la carte de jeu (CJI) par rapport aux données (SI) lues dans la base de données (BD) afin de contrôler l'intégrité de la carte de jeu (CJ1). revendications
 - des 1'une selon Procédě ce que l'étape précédentes, caractérisé en vérification consiste à :
 - vérifier le numéro d'identification (Id) de la carte de jeu (CJ1) avec une clé d'identification (Kt1) lue dans la base de données (BD) de l'organe central de

5

10

15

20

25

30

gestion (1) afin de contrôler l'intégrité de la carte de jeu (CJ1).

- Procédé salon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation (MSO), le procédé comportant une étape supplémentaire consistant à :
- prévoir que les moyens de sécurisation (MSO) du réseau calculent un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des moyens de sécurisation.
- Procédé salon la revendication 7, caractérisé par une étape supplémentaire consistant à :
- lire un certificat d'authentification calculé par la carte de jeu (CJI) à partir de données sacrètes (Kt, Kt1) an mémoire de la carte.
- Procédé selon la revendication 8 caractérisé en ce que l'étape de vérification consiste à :
- vérifier que le certificat d'authentification (C) calculé par la carte de jeu (CJ1) correspond au certificat d'authentification (C') calculé par les moyens de sécurisation (MSO) du réseau.
- 10. Procédé selon l'une des revendications précédentes caractérisé en ce que la réseau comporte en outre des moyens de sécurisation répartis (MSO, MS1), le procédé comportant des écapes supplémentaires consistant à :
- prévoir que des premiers moyens de sécurisation du réseau calculent un premier certificat d'authentification (C') à partir de données secrètes Kt') en mémoire des premiers moyens (Kt. sécurisation (MSO), et
- prévoir que des seconds moyens de sécurisation second certificat du réseau calculent un d'authentification à partir de données secrêtes en mémoire des seconds moyens de sécurisation (MS1), et

WO 98/47113

5

10

15

20

25

JO

- vérifier que le premier certificat d'authentification (C') calculé par les premiers moyens de sécurisation (MSO) du réseau correspond au second certificat d'authentification calculé par les seconds moyens de sécurisation (MSI) du réseau.
- 11. Procêdé selon l'une des revendications 7 à 10 caractérisé en ce que les données (Id, 5) échangées entre la machine (200) et la base de données (BD) de l'organe central de gestion (1) sont accompagnées d'un certificat d'authentification (C, C').
- 12. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés au transcripteur (T, 10, 110, 210) de données sur carte de jeu (CJ1) afin de contrôler l'intégrité d'une telle carte.
- 13. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés à une machine de jeu (T, 200, 300).
- 14. Procêdé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation sont associés aux moyens de liaison du réseau.
 - 15. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MSO) sont associés à l'organe central de gestion (1) afin de contrôler l'intégrité du réseau.
 - transferts de contrôle de sácurisé Système d'unités de valeur entre une pluralité de cartes de jeu (CJ) et une pluralité de machines de jeu (200, 300), chaque machine étant pourvue d'un transcripteur (210, 310) apte à débiter des unités de valeur d'une carte de jeu (CJ), les machines étant reliées en réseau sécurisé gestion (1) central de organe цn l'intermédiaire de moyens de liaison (123), une carte de jeu (CJ1) stockant en mémoire des données (S, Op1,

WO 98/47113

5

25

représentatives d'opérations jeu Opx) effectuées, notamment des données d'identification (Id) op2, de la carte et des données représentatives de solde (S) des unités de valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion (1) comporte une base de données (BD) stockant parallèlement en mémoire les données (S1, Opioi, Opioi, Opiox) représentatives des opérations de jeu effectuées, notamment les données d'identification (Id1, Id2, Idn) des cartes et les données représentatives des soldes (S1, S2, Sn) des 10 unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens vérifient que, pour une carte de contrôle (BD) identifiée, les données de la base (ED) et les données de la carte (CJ1) correspondent, notamment que les 15 connées (S. Sl) représentatives du solde d'unités de valeur correspondent, afin de vérifier l'intégrité du système. revendication la

- 17. Système sécurisé selon caractérisé en ce que la carte de jeu (CJ1) calcule un 20 certificat d'authentification (C) à partir de données secràtes (Kt. Kt') stockées en mémoire de la carte
- 18. Système sécurisé selon la revendication 16 ou la revendication 17, caractérisé en ce qu'il comporte en 25 outre au moins un module de sécurisation (MSO, MS1), le sécurisation calculant d'anthentification (C') à partir de données secrètes module (Kt. Kt') stockées en mémoire du module (MSO) et en ce que les moyens de contrôle (MSO) vérifient que le 30 (C') calculé certificat d'authentification au certificat module de sécurisation correspond

WO 98/47113

20

26

d'authentification (C') calculé par la carte de jeu ou par un autre module de sécurisation (MS1).

- par un autre module de selon la revendication 18, 19. Système sécurisé selon la revendication (MSL) caractérisé en ce qu'un module de sécurisation (MSL) est disposé dans le transcripteur (T, 10, 210, 310).
- est dispose dans le clambour d'une des revendications 18 20. Système sécurisé selon l'une des revendications 18 et 19, caractérisé en ce qu'un module de sécurisation (MSO) est disposé dans une machine de jeu (200).
- 21. Système sécurisé selon l'une des revendications 18
 10 à 20, caractérisé en ce qu'un module de sécurisation est disposé sur les moyens de liaison du réseau.
 - 22. Système sécurisé selon l'une des revendications 18 à 21, caractérisé en ce qu'un module de sécurisation (MSO) est disposé dans l'organe central de gestion (1).
- 15 2]. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte à puce.
 - 24. Procédé cu système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte sans contact.
 - 25. Procédé ou système sécurisé selon l'une des revendications précédentes caractérisé en ce qu'une carte de jeu est une carte bancaire.



1/2

